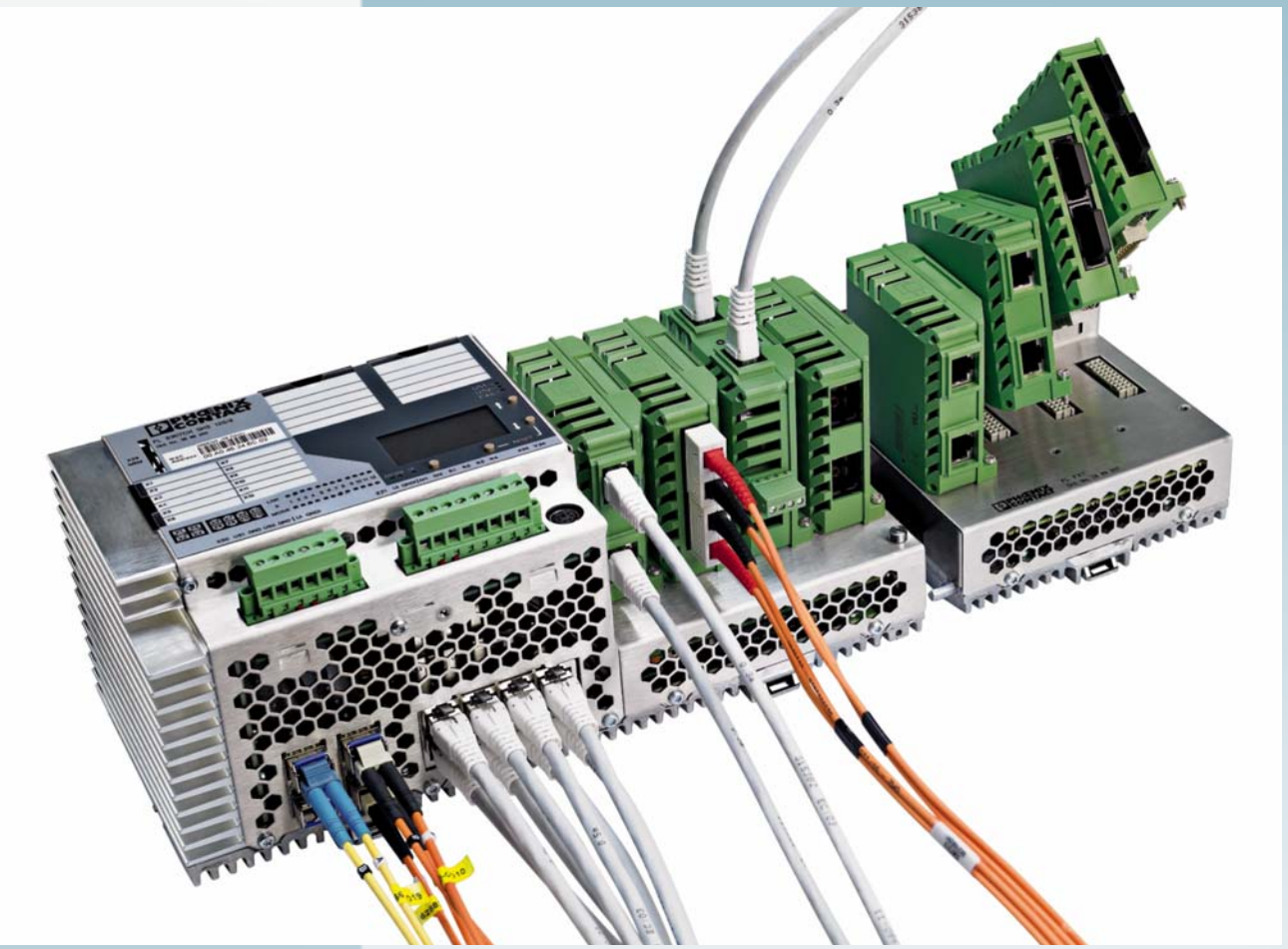
AUTOMATION



User Manual

UM EN FL SWITCH GHS CLI for

FL SWITCH GHS 12G/8

FL SWITCH GHS 4G/12

Gigabit Modular Switch

Order No: -

PHOENIX CONTACT

INSPIRING INNOVATIONS

AUTOMATION

User Manual

Description of the CLI interface of the Gigabit Modular Switches

10/2010

Designation: UM EN FL SWITCH GHS CLI

Revision: 01

Order No: —

This user manual is valid for:

Designation	Revision	Order No:
FL SWITCH GHS		2989200
FL SWITCH GHS 4G/12		2700271
FL FXT		2989307

Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this manual.

User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER
This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION
This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

The following types of messages provide information about possible property damage and general information concerning proper operation and ease-of-use.

NOTE
This symbol and the accompanying text alerts the reader to a situation which may cause damage or malfunction to the device, either hardware or software, or surrounding property.

This symbol and the accompanying text provides additional information to the reader. It is also used as a reference to other sources of information (manuals, data sheets, literature) on the subject matter, product, etc.

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of legal authority

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:

www.phoenixcontact.com.

Make sure you always use the latest documentation.
It can be downloaded at:

www.phoenixcontact.net/catalog.

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at www.phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
Germany
Phone +49 - (0) 52 35 - 3-00
Fax +49 - (0) 52 35 - 3-4 12 00

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to

tecdoc@phoenixcontact.com.

01Table of Content

Section 1: Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **`show network`** or **`clear vlan,`** do not require parameters. Other commands, such as **`network parms`**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **`network parms`** command syntax:

Format **`network parms`** *`<ipaddr> <netmask> [gateway]`*

- **`network parms`** is the command name.
- *`<ipaddr>`* and *`<netmask>`* are parameters and represent required values that you must enter after you type the command keywords.
- *`[gateway]`* is an optional parameter, so you are not required to enter a value in place of the parameter.

The *CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **`show`** commands also contain a description of the information that the command shows.

COMMAND CONVENTIONS

In this document, the command name is in **`bold`** font. Parameters are in *`italic font`*. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. Table 1 describes the conventions this document uses to distinguish between value types.

Table 1: ***Parameter Conventions***

Symbol	Example	Description
<> angle brackets	*<value>*	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	*[value]*	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} curly braces	*{choice1 | choice2}*	Indicates that you must select a parameter from the list of choices.
| Vertical bars	*choice1 | choice2*	Separates the mutually exclusive choices.
[{}] Braces within square brackets	*[{choice1 | choice2}]*	Indicates a choice within an optional element.

COMMON PARAMETER VALUES

Parameter values might be names (strings) or numbers.To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 2 describes common parameter values and value formatting.

Table 2: ***Parameter Descriptions***

Parameter	Description

ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats:
	`a (32 bits)`
	`a.b (8.24 bits)`
	`a.b.c (8.8.16 bits)`
	`a.b.c.d (8.8.8.8)`
	In addition to these formats, the CLI accepts decimal, hexidecimal and octal formats through the following input formats (where *n* is any valid hexidecimal, octal or decimal number):
	`0xn (CLI assumes hexidecimal format)`
	`0n (CLI assumes octal format with leading zeros)`
	`n (CLI assumes decimal format)`

ipv6-address	`FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or`
	`FE80:0:0:0:20F:24FF:FEBF:DBCB, or`
	`FE80::20F24FF:FEBF:DBCB, or`
	`FE80:0:0:0:20F:24FF:128:141:49:32`
	For additional information, refer to RFC 3513.

Interface or slot/port	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

SLOT/PORT NAMING CONVENTION

FL SWITCH GHS Firmware software references physical entities such as cards and ports by using a slot/port naming convention. The FL SWITCH GHS Firmware software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 3: ***Type of Slots***

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4: ***Type of Ports***

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Note: In the CLI, loopback and tunnel interfaces do not use the slot/port format. To specify a loopback interface, you use the loopback ID. To specify a tunnel interface, you use the tunnel ID.

USING THE "NO" FORM OF A COMMAND

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form to reverse the action of a command or reset a value back to the default. For example, the **no shutdown** configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the **no** form.

FL SWITCH GHS FIRMWARE MODULES

FL SWITCH GHS Firmware software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some **show** commands, the output fields might change based on the modules included in the FL SWITCH GHS Firmware software.

The FL SWITCH GHS Firmware software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- IPv6—IPv6 routing
- Multicast
- BGP-4
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- IPv6 Management—Allows management of the FL SWITCH GHS Firmware device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in

the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN) and the Service port.

- WLAN Switching (4.4.2 and later)
- Stacking

Not all modules are available for all platforms or software releases.

COMMAND MODES

The CLI groups commands into modes according to the command function. Each of the command modes supports specific FL SWITCH GHS Firmware software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 5 describes the command modes and the prompts visible in that mode.

Note: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the Router BGPv4 Command Mode.

Table 5: ***CLI Command Modes***

Command Mode	Prompt	Mode Description
User EXEC	`Switch>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`Switch#`	Allows you to issue any **`EXEC`** command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`Switch (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`Switch (Vlan)#`	Groups all the VLAN commands.

Interface Config	`Switch (Interface <slot/port>)#`
	`Switch (Interface Loopback <id>)#`
	`Switch (Interface Tunnel <id>)#`
		Manages the operation of an interface and provides access to the router interface configuration commands.
		Use this mode to set up a physical port for a specific logical connection operation.

Line Config	`Switch (line)#`	Contains commands to configure outbound telnet settings and console interface settings.
Policy Map Config	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class Config	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv4.

Table 5: ***CLI Command Modes (Cont.)***

Command Mode	Prompt	Mode Description
Ipv6_Class-Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv6.
Router OSPF Config	`Switch (Config-router)#`	Contains the OSPF configuration commands.
Router OSPFv3 Config	`Switch (Config rtr)#`	Contains the OSPFv3 configuration commands.
Router RIP Config	`Switch (Config-router)#`	Contains the RIP configuration commands.
Router BGP Config	`Switch (Config-router)#`	Contains the BGP4 configuration commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	`Switch (Config dhcp-pool)#`	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	`Switch (Config dhcp6-pool)#`	Contains the DHCPv6 server IPv6 address pool configuration commands.
Wireless Config Mode	`Switch (Config-wireless)#`	Contains global WLAN switch configuration commands and provides access to other WLAN command modes.
AP Config Mode	`Switch (Config-ap)#`	Contains commands to configure entries in the local AP database, which is used for AP validation.
AP Profile Config Mode	`Switch (Config-ap-profile)#`	Contains commands to configure the default AP profile settings as well as settings for new AP profile.
AP Profile Radio Config Mode	`Switch (Config-ap-profile-radio)#`	Contains commands to modify the radio configuration parameters for an AP profile.
AP Profile VAP Config Mode	`Switch (Config-ap-profile-vap)#`	Contains commands to configure radio 1 or radio 2 within an AP profile.
Network Config Mode	`Switch (Config-network)#`	Contains commands to configure WLAN settings for up to 64 different networks.

Table 6 explains how to enter or exit each mode.

Table 6: ***CLI Mode Access and Exit***

Command Mode	Access Method	Exit or Access Previous Mode
User EXEC	This is the first level of access.	To exit, enter **`logout`**.
Privileged EXEC	From the User EXEC mode, enter **`enable`**.	To exit to the User EXEC mode, enter **`exit`** or press **`Ctrl-Z.`**
Global Config	From the Privileged EXEC mode, enter **`configure.`**	To exit to the Privileged EXEC mode, enter **`exit`**, or press **`Ctrl-Z`**.
VLAN Config	From the Privileged EXEC mode, enter **`vlan database.`**	To exit to the Privileged EXEC mode, enter **`exit`**, or press **`Ctrl-Z`**.

Table 6: ***CLI Mode Access and Exit (Cont.)***

Command Mode	Access Method	Exit or Access Previous Mode
Interface Config	From the Global Config mode, enter **interface** *<slot/port>* or **interface loopback** *<id>* or **interface tunnel** *<id>*	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Line Config	From the Global Config mode, enter **lineconfig**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Policy-Map Config	From the Global Config mode, enter **policy-map**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Policy-Class-Map Config	From the Policy Map mode enter **class**.	To exit to the Policy Map mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Class-Map Config	From the Global Config mode, enter **class-map**, and specify the optional keyword *ipv4* to specify the Layer 3 protocol for this class. See "class-map" on page 8 for more information.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Ipv6-Class-Map Config	From the Global Config mode, enter **class-map** and specify the optional keyword *ipv6* to specify the Layer 3 protocol for this class. See "class-map" on page 8 for more information.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Router OSPF Config	From the Global Config mode, enter **router ospf**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Router OSPFv3 Config	From the Global Config mode, enter **ipv6 router ospf**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Router RIP Config	From the Global Config mode, enter **router rip**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Router BGP Config	From the Global Config mode, enter **router bgp** *<asnumber>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
MAC Access-list Config	From the Global Config mode, enter **mac access-list extended** *<name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
TACACS Config	From the Global Config mode, enter **tacacs-server host** *<ip-addr>*, where *<ip-addr>* is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
DHCP Pool Config	From the Global Config mode, enter **ip dhcp pool** *<pool-name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
DHCPv6 Pool Config	From the Global Config mode, enter **ip dhcpv6 pool** *<pool-name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Wireless Config Mode	From the Global Config mode, enter **wireless**.	To exit to Global Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
AP Config Mode	From the Wireless Config mode, enter **ap database** *<macaddr>*, where *<macaddr>* is the MAC address of the AP to configure..	To exit to Wireless Config mode, enter **exit**. To return to the User EXEC mode, enter **Ctrl-Z**.
AP Profile Config Mode	From the Wireless Config mode, enter **ap profile** *<1-16>*, where *<1-16>* is the profile ID.	To exit to Wireless Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
AP Profile Radio Config Mode	From the AP Profile Config mode, enter **radio** *<1-2>*.	To exit to AP Profile Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.

Table 6: ***CLI Mode Access and Exit (Cont.)***

Command Mode	Access Method	Exit or Access Previous Mode
AP Profile VAP Config Mode	From the AP Profile Radio Config mode, enter **vap** *<0-7>*, where *<0-7>* is the VAP ID.	To exit to AP Profile Radio Configmode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
Network Config Mode	From the Wireless Config mode, enter **network** *<1-64>*, where *<1-64>* is the network ID.	To exit to Wireless Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.

COMMAND COMPLETION AND ABBREVIATION

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7 describes the most common CLI error messages.

Table 7: *CLI Error Messages*

Message Text	Description
`% Invalid input detected at '^' marker.`	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
`Command not found / Incomplete command. Use ? to list commands.`	Indicates that you did not enter the required keywords or values.
`Ambiguous command`	Indicates that you did not enter enough letters to uniquely identify the command.

CLI Line-Editing Conventions

Table 8 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering **`help`** from the User or Privileged EXEC modes.

Table 8: *CLI Editing Conventions*

Key Sequence	Description
DEL or Backspace	Delete previous character
Ctrl-A	Go to beginning of line
Ctrl-E	Go to end of line
Ctrl-F	Go forward one character
Ctrl-B	Go backward one character
Ctrl-D	Delete current character
Ctrl-U, X	Delete to beginning of line
Ctrl-K	Delete to end of line
Ctrl-W	Delete previous word
Ctrl-T	Transpose previous character
Ctrl-P	Go to previous line in history buffer
Ctrl-R	Rewrites or pastes the line
Ctrl-N	Go to next line in history buffer
Ctrl-Y	Prints last deleted character
Ctrl-Q	Enables serial flow
Ctrl-S	Disables serial flow
Ctrl-Z	Return to root command prompt
Tab, <SPACE>	Command-line completion

Table 8: ***CLI Editing Conventions (Cont.)***

Key Sequence	Description
Exit	Go to next lower command prompt
?	List available commands, keywords, or parameters

USING CLI HELP

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(switch) >?

enable                    Enter into user privilege mode.
help                      Display help for various special keys.
logout                Exit this session. Any unsaved changes are lost.
ping                 Send ICMP echo packets to a specified IP address.
quit                  Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(switch) #network ?

javamode                  Enable/Disable.
mgmt_vlan              Configure the Management VLAN ID of the switch.
parms                     Configure Network Parameters of the router.
protocol                  Select DHCP, BootP, or None as the network
config
                          protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(switch) #network parms ?

<ipaddr>                  Enter the IP address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                      Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(switch) #show m?

mac-addr-table            mac-address-table        monitor
```

ACCESSING THE CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see “Network Interface Commands” on page 1.

Section 2: Switching Commands

This chapter describes the switching commands available in the FL SWITCH GHS Firmware CLI.

Caution! The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

PORT CONFIGURATION COMMANDS

This section describes the commands you use to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

Format `interface` *<slot/port>*
Mode Global Config

Format `interface` *<slot/port>*
Mode Global Config

AUTO-NEGOTIATE

This command enables automatic negotiation on a port.

Default enabled
Format `auto-negotiate`
Mode Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Note: Automatic sensing is disabled when automatic negotiation is disabled.

Format `no auto-negotiate`
Mode Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default enabled
Format `auto-negotiate all`
Mode Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format `no auto-negotiate all`
Mode Global Config

description

Use this command to create an alpha-numeric description of the port.

Format `description` *<description>*
Mode Interface Config

mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard FL SWITCH GHS Firmware implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see "ip mtu" on page 143.

Default 1518 (untagged)
Format `mtu` *<1518-9216>*
Mode Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format `no mtu`

Mode Interface Config

shutdown

This command disables a port.

Note: You can use the **`shutdown`** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default enabled

Format **`shutdown`**

Mode Interface Config

no shutdown

This command enables a port.

Format **`no shutdown`**

Mode Interface Config

shutdown all

This command disables all ports.

Note: You can use the **`shutdown all`** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default enabled

Format **`shutdown all`**

Mode Global Config

no shutdown all

This command enables all ports.

Format **`no shutdown all`**

Mode Global Config

speed

This command sets the speed and duplex setting for the interface.

Format **`speed`** *{<100 | 10> <half-duplex | full-duplex>}*

Mode Interface Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

speed all

This command sets the speed and duplex setting for all interfaces.

Format **`speed all`** *{<100 | 10> <half-duplex | full-duplex>}*

Mode Global Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

show port

This command displays port information.

Format **`show port`** *{<slot/port> | all}*

Mode Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** - this port is a monitoring port. For more information, see "Port Mirroring" on page 65. • **PC Mbr**- this port is a member of a port-channel (LAG). • **Probe** - this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.

Term	Definition
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format `show port protocol {<groupid> | all}`

Mode Privileged EXEC

Term	Definition
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
Protocol(s)	The type of protocol(s) for this group.
VLAN	The VLAN associated with this Protocol Group.
Interface(s)	Lists the slot/port interface(s) that are associated with this Protocol Group.

SPANNING TREE PROTOCOL (STP) COMMANDS

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note: STP is disabled by default. When you enable STP on the switch, STP is still disabled on each port.

Note: If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default disabled

Format `spanning-tree`

Mode Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format `no spanning-tree`
Mode Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on the interface.

Default disabled
Format `spanning-tree bpdufilter`
Mode Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface.

Default disabled
Format `no spanning-tree bpdufilter`
Mode Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default disabled
Format **`spanning-tree bpdufilter`**
Mode Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default disabled
Format **`no spanning-tree bpdufilter default`**
Mode Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

Default disabled
Format **`spanning-tree bpduflood`**
Mode Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

Default disabled
Format **`no spanning-tree bpduflood`**
Mode Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default disabled
Format **`spanning-tree bpduguard`**
Mode Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default disabled
Format **`no spanning-tree bpduguard`**
Mode Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *<slot/port>* parameter to transmit a BPDU from a specified interface, or use the *all* keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a “no” version.

Format **`spanning-tree bpdumigrationcheck`** *{<slot/port> | all}*
Mode Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *<name>* is a string of up to 32 characters.

Default base MAC address in hexadecimal notation
Format **`spanning-tree configuration name`** *<name>*
Mode Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`

Mode Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default 0

Format `spanning-tree configuration revision` *<0-65535>*

Mode Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format `no spanning-tree configuration revision`

Mode Global Config

spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format `spanning-tree edgeport`

Mode Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format `no spanning-tree edgeport`

Mode Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default 802.1s

Format `spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*

Mode Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format `no spanning-tree forceversion`

Mode Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default 15

Format `spanning-tree forward-time <4-30>`

Mode Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree forward-time`

Mode Global Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time `<value>` is in whole seconds within a range of 1 to 10, with the value being less than or equal to *(Bridge Max Age / 2) - 1*.

Default 2

Format `spanning-tree hello-time <1-10>`

Mode Interface Config

no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree hello-time`

Mode Interface Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default 20

Format `spanning-tree max-age <6-40>`

Mode Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree max-age`

Mode Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default 20

Format `spanning-tree max-hops <1-127>`

Mode Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree max-hops`

Mode Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **external-cost** option, this command sets the external-path cost for MST instance '0' i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify auto, the external path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default
- cost—auto
- external-cost—auto
- port-priority—128

Format **spanning-tree mst <***mstid> {{cost <1-200000000> | auto} | {external-cost <1-200000000> | auto} | port-priority <0-240>}*

Mode Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst '0' instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value.

Format **no spanning-tree mst** *<mstid> <cost | external-cost | port-priority>*

Mode Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter *<mstid>* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default none

Format **spanning-tree mst instance** *<mstid>*

Mode Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format **no spanning-tree mst instance** *<mstid>*

Mode Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default 32768

Format **spanning-tree mst priority** *<mstid> <0-61440>*

Mode Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *<mstid>*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format **no spanning-tree mst priority** *<mstid>*

Mode Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN so that the VLAN is no longer associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format **spanning-tree mst vlan** *<mstid> <vlanid>*

Mode Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN so that the VLAN is again be associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format **no spanning-tree mst vlan** *<mstid> <vlanid>*

Mode Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default disabled

Format **spanning-tree port mode**

Mode Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format **no spanning-tree port mode**

Mode Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default disabled

Format `spanning-tree port mode all`

Mode Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format `no spanning-tree port mode all`

Mode Global Config

spanning-tree rootguard

Use this command to enable root BPDU Guard on the interface.

Default disabled

Format `spanning-tree rootguard`

Mode Interface Config

no spanning-tree rootguard

Use this command to disable root BPDU Guard on the interface.

Format `no spanning-tree rootguard`

Mode Interface Config

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.

Term	Definition
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. The following details are displayed on execution of the command.

Format **show spanning-tree interface** *<slot/port>*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Filter	Enabled or disabled.
BPDU Flood	Enabled or disabled.
BPDU Guard	Enabled or disabled.
Root Guard	Enabled or disabled.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RST BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<slot/port>* is the desired switch port.

Format **show spanning-tree mst port detailed** *<mstid> <slot/port>*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The ID of the existing MST instance.

Term	Definition
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	Configured value of the external Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. In this case, the following are displayed.

Term	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Port Path Cost	The configured path cost for the specified interface.
Designated Root	Identifier of the designated root for this port within the CST.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.

Term	Definition
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Port Cost	The configured path cost for this port.

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *<mstid>* indicates a particular MST instance. The parameter {*<slot/port>* | *all*} indicates the desired switch port or all ports.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format **`show spanning-tree mst port summary`** *<mstid> {<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	Valid slot and port number separated by a forward slash.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Link Status	The operational status of the link. Possible values are “Up” or “Down”.
Link Trap	The link trap configuration for the specified interface.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format **`show spanning-tree mst summary`**

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	Identifier used to identify the configuration currently being used.
MST Instances	List of all multiple spanning tree instances configured on the switch.

show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format `show spanning-tree vlan` *<vlanid>*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN Identifier	The VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.

VLAN COMMANDS

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format **`vlan database`**

Mode Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default 1

Format **`network mgmt_vlan`** *`<1-4069>`*

Mode Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format **`no network mgmt_vlan`**

Mode Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4094.

Format **`vlan`** *`<2-4094>`*

Mode VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4094.

Format **`no vlan`** *`<2-4094>`*

Mode VLAN Config

vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and

assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default all

Format **vlan acceptframe** *{vlanonly | all}*

Mode Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface to the default value.

Format **no vlan acceptframe**

Mode Interface Config

vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled

Format **vlan ingressfilter**

Mode Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format **no vlan ingressfilter**

Mode Interface Config

vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4094.

Format **vlan makestatic** *<2-4094>*

Mode VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4094.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name <2-4094> <name>`

Mode VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name <2-4094>`

Mode VLAN Config

vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format `vlan participation {exclude | include | auto} <1-4094>`

Mode Interface Config

Participation options are:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format `vlan participation all {exclude | include | auto} <1-4094>`

Mode Global Config

You can use the following participation options:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.

Participation Options	Definition
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

Format **`vlan port acceptframe all`** *{vlanonly | all}*

Mode Global Config

The modes defined as follows:

Mode	Definition
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format **`no vlan port acceptframe all`**

Mode Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled

Format **`vlan port ingressfilter all`**

Mode Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan port ingressfilter all`

Mode Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default 1

Format `vlan port pvid all <1-4094>`

Mode Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format `no vlan port pvid all`

Mode Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan port tagging all <1-4094>`

Mode Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan port tagging all`

Mode Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The *<groupName>* is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format **vlan protocol group** *<groupname>*
Mode Global Config

vlan protocol group add protocol

This command adds the *<protocol>* to the protocol-based VLAN identified by *<groupid>*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for protocol are *ip, arp,* and *ipx*.

Note: FL SWITCH GHS Firmware software supports IPv4 protocol-based VLANs.

Default none
Format **vlan protocol group add protocol** *<groupid> <protocol>*
Mode Global Config

no vlan protocol group add protocol

This command removes the *<protocol>* from this protocol-based VLAN group that is identified by this *<groupid>*. The possible values for protocol are *ip, arp,* and *ipx*.

Format **no vlan protocol group add protocol** *<groupid> <protocol>*
Mode Global Config

vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this *<groupid>*.

Format **vlan protocol group remove** *<groupid>*
Mode Global Config

protocol group

This command attaches a *<vlanid>* to the protocol-based VLAN identified by *<groupid>*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default none
Format **protocol group** *<groupid> <vlanid>*
Mode VLAN Config

no protocol group

This command removes the *<vlanid>* from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **no protocol group** *<groupid> <vlanid>*

Mode VLAN Config

protocol vlan group

This command adds the physical interface to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default none

Format **protocol vlan group** *<groupid>*

Mode Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **no protocol vlan group** *<groupid>*

Mode Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default none

Format **protocol vlan group all** *<groupid>*

Mode Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **no protocol vlan group all** *<groupid>*

Mode Global Config

vlan pvid

This command changes the VLAN ID per interface.

Default 1

Format **vlan pvid** *<1-4094>*

Mode Interface Config

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format **no vlan pvid**

Mode Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format **vlan tagging** *<1-4094>*

Mode Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format **no vlan tagging** *<1-4094>*

Mode Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format **vlan association subnet** *<ipaddr> <netmask> <vlanid>*

Mode VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format **no vlan association subnet** *<ipaddr> <netmask>*

Mode VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format **vlan association mac** *<macaddr> <vlanid>*

Mode VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format **no vlan association mac** *<macaddr>*

Mode VLAN database

vlan tagging mode

Default transparent

Format **vlan database mode tagging**

Mode Privileged EXEC

Default transparent

Format **vlan database mode transparent**

Mode Privileged EXEC

show vlan mode

Format **show vlan mode** *<cr>*

Mode VLAN database

show vlan

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

Format **show vlan** *<vlanid>*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.

Term	Definition
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** - Transmit traffic for this VLAN as tagged frames. • **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format `show vlan port` *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format `show vlan association subnet` *[<ipaddr> <netmask>]*

Mode Privileged EXEC

Term	Definition
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format `show vlan association mac` *[<macaddr>]*

Mode Privileged EXEC

Term	Definition
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

PROVISIONING (IEEE 802.1P) COMMANDS

This section describes the commands you use to configure provisioning, which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format `vlan port priority all` *<priority>*

Mode Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default 0

Format `vlan priority` *<priority>*

Mode Interface Config

GARP COMMANDS

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and Garp Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time for one port (Interface Config mode) or all (Global Config mode) and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default 20

Format **`set garp timer join`** *`<10-100>`*

Mode
- Interface Config
- Global Config

no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default and only has an effect when GVRP is enabled.

Format **`no set garp timer join`**

Mode
- Interface Config
- Global Config

set garp timer leave

This command sets the GVRP leave time for one port (Interface Config mode) or all ports (Global Config mode) and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Default 60

Format **`set garp timer leave`** *`<20-600>`*

Mode
- Interface Config
- Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format **`no set garp timer leave`**

Mode
- Interface Config
- Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode) or a single port (Interface Config mode), and it only has an effect only when GVRP is enabled.

Default 1000

Format `set garp timer leaveall <200-6000>`

Mode
- Interface Config
- Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format `no set garp timer leaveall`

Mode
- Interface Config
- Global Config

show garp

This command displays GARP information.

Format `show garp`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP COMMANDS

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note: If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default disabled

Format `set gvrp adminmode`

Mode Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format `no set gvrp adminmode`

Mode Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode) or all ports (Global Config mode).

Default disabled

Format `set gvrp interfacemode`

Mode
- Interface Config
- Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format `no set gvrp interfacemode`

Mode
- Interface Config
- Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format `show gvrp configuration` *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

Term	Definition
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP COMMANDS

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note: If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default disabled

Format `set gmrp adminmode`

Mode Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format `no set gmrp adminmode`

Mode Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode) or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default disabled

Format `set gmrp interfacemode`

Mode
- Interface Config
- Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format `no set gmrp interfacemode`

Mode
- Interface Config
- Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format `show gmrp configuration` *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table gmrp`

Mode Privileged EXEC

Term	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

PORT-BASED NETWORK ACCESS CONTROL COMMANDS

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format `clear dot1x statistics` *{<slot/port> | all}*

Mode Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format `clear radius statistics`

Mode Privileged EXEC

dot1x guest-vlan

This command configures VLAN as guest vlan on a per port basis. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximumVLAN ID supported by the platform.

Default disabled

Format **dot1x guest-vlan** *<vlan-id>*

Mode Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default disabled

Format **no dot1x guest-vlan**

Mode Interface Config

dot1x guest-vlan supplicant

This command configures Guest VLAN to be assigned to supplicants that have failed authentication.

Default disabled

Format **dot1x guest-vlan supplicant**

Mode Global Config

no dot1x guest-vlan supplicant

This command disables Guest VLAN supplicant on the switch.

Default disabled

Format **no dot1x guest-vlan supplicant**

Mode Global Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format **dot1x initialize** *<slot/port>*

Mode Privileged EXEC

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *<count>* value must be in the range 1 - 10.

Default 2

Format **dot1x max-req** *<count>*

Mode Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format **no dot1x max-req**

Mode Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified port. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default auto

Format **dot1x port-control** *{force-unauthorized | force-authorized | auto}*

Mode Interface Config

no dot1x port-control

This command sets the authentication mode on the specified port to the default value.

Format **no dot1x port-control**

Mode Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default auto

Format **dot1x port-control all** *{force-unauthorized | force-authorized | auto}*

Mode Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format `no dot1x port-control all`

Mode Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format `dot1x re-authenticate` *<slot/port>*

Mode Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default disabled

Format `dot1x re-authentication`

Mode Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format `no dot1x re-authentication`

Mode Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default disabled

Format `dot1x system-auth-control`

Mode Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format `no dot1x system-auth-control`

Mode Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default
- reauth-period: 3600 seconds
- quiet-period: 60 seconds
- tx-period: 30 seconds
- supp-timeout: 30 seconds
- server-timeout: 30 seconds

Format **`dot1x timeout`** *{{reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}*

Mode Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format **`no dot1x timeout`** *{reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}*

Mode Interface Config

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format **show dot1x** *[{summary {<slot/port> | all} | detail <slot/port> | statistics <slot/port>]*

Mode Privileged EXEC

If you do not use the optional parameters *<unit/slot/port>* or *<vlanid>*, the command displays the global dot1x mode and the Guest VLAN supplicant mode.

Term	Definition
Administrative mode	Indicates whether authentication control on the switch is enabled or disabled.
Supplicant Allowed in Guest VLAN	Indicates whether Guest VLAN is enabled or disabled.

If you use the optional parameter *summary {<slot/port> | all}*, the dot1x configuration for the specified port or all ports are displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized	force-authorized	auto.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized	unauthorized.
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port.

The command **show dot1x detail** *<unit/slot/port>* displays guest-vlan. The configured guest-vlan ID is displayed. If the optional parameter '**detail** *<slot/port>*' is used, the detailed dot1x configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Term	Definition
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest-Vlan Operational Mode	Indicates whether guest-vlan operational mode is enabled or disabled.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Vlan-assigned	The VLAN assigned to the port by the radius server.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.

If you use the optional parameter **`statistics`** *<slot/port>*, the following dot1x statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.

Term	Definition
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

STORM-CONTROL COMMANDS

This section describes commands you use to configure storm control and view storm-control configuration information. The Storm Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis. The Storm Control feature can help maintain network performance.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control broadcast`

Mode Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface.

Format `no storm-control broadcast`

Mode Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold in terms of percentage of the interface speed for an interface. When you use this command, broadcast storm recovery mode is enabled on the interface and broadcast storm recovery is active. If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 5

Format `storm-control broadcast level` *<0-100>*

Mode Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format `no storm-control broadcast level`

Mode Interface Config

storm-control broadcast all

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control broadcast all`

Mode Global Config

no storm-control broadcast all

This command disables broadcast storm recovery mode for all interfaces.

Format `no storm-control broadcast all`

Mode Global Config

storm-control broadcast all level

This command configures the broadcast storm recovery threshold in terms of percentage of the interface speed for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.This command also enables broadcast storm recovery mode for all interfaces.

Default 5

Format `storm-control broadcast all level` *<0-100>*

Mode Global Config

no storm-control broadcast all level

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format `no storm-control broadcast all level`

Mode Global Config

storm-control multicast

This command enables multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast`

Mode Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format `no storm-control multicast`

Mode Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold in terms of percentage of the interface speed for an interface and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast level` *<0-100>*

Mode Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format `no storm-control multicast level` *<0-100>*

Mode Interface Config

storm-control multicast all

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast all`

Mode Global Config

no storm-control multicast all

This command disables multicast storm recovery mode for all interfaces.

Format `no storm-control multicast all`

Mode Global Config

storm-control multicast all level

This command configures the multicast storm recovery threshold, in terms of percentage of the interface speed, for all interfaces and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast all level` *<0-100>*

Mode Global Config

no storm-control multicast all level

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Format `no storm-control multicast all level`

Mode Global Config

storm-control unicast

This command enables unicast storm recovery mode for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control unicast`

Mode Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format `no storm-control unicast`

Mode Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold in terms of percentage of the interface speed for an interface, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default 5

Format `storm-control unicast level` *<0-100>*

Mode Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format `no storm-control unicast level`

Mode Interface Config

storm-control unicast all

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control unicast all`

Mode Global Config

no storm-control unicast all

This command disables unicast storm recovery mode for all interfaces.

Format `no storm-control unicast all`

Mode Global Config

storm-control unicast all level

This command configures the unicast storm recovery threshold in terms of percentage of the interface speed for an interface, and enables unicast storm recovery for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control unicast all level` *<0-100>*

Mode Global Config

no storm-control unicast all level

This command returns the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

Format `no storm-control unicast all level`

Mode Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.

Note: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default disabled

Format `storm-control flowcontrol`

Mode Global Config

no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Format `no storm-control flowcontrol`

Mode Global Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters. Use the **all** keyword to display the per-port configuration parameters for all interfaces, or specify the *slot/port* to display information about a specific interface.

Format **show storm-control** *[all | <slot/port>]*

Mode Privileged EXEC

Term	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

PORT-CHANNEL/LAG (802.3AD) COMMANDS

This section describes the commands you use to configure port-channels, which are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The *<name>* field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the **show port channel** command to display the slot/port number for the logical interface.

Note: Before you include a port in a port-channel, set the port physical mode. For more information, see "speed" on page 3.

Format `port-channel <name>`
Mode Global Config

no port-channel

This command deletes a port-channel (LAG).

Format `no port-channel {<logical slot/port> | all}`
Mode Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 3.

Format `addport <logical slot/port>`
Mode Interface Config

deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel.

Format `deleteport <logical slot/port>`
Mode Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel. To clear the port channels, see "clear port-channel" on page 22.

Format `deleteport {<logical slot/port> | all}`
Mode Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of <*key*> is 0 to 65535.

Default 0x8000
Format `lacp admin key <key>`

Mode Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format `no lacp admin key`

Mode Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. The valid range of <*delay*> is 0-65535.

Default 0x8000

Format `lacp collector max delay <delay>`

Mode Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format `no lacp collector max delay`

Mode Interface Config

lacp actor admin

Use this command to configure the LACP actor admin parameters.

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key. The valid range for <*key*> is 0-65535.

Default Internal Interface Number of this Physical Port

Format `lacp actor admin key <key>`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format `no lacp actor admin key`
Mode Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. The valid value range is 0x00-0xFF.

Default 0x07
Format `lacp actor admin state {individual|longtimeout|passive}`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Format `no lacp actor admin state {individual|longtimeout|passive}`
Mode Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format `lacp actor admin state individual`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format `no lacp actor admin state individual`
Mode Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format `lacp actor admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format `no lacp actor admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format `lacp actor admin state passive`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format `no lacp actor admin state passive`
Mode Interface Config

lacp actor port

Use this command to configure LACP actor port priority key.

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port. The valid range for <*priority*> is 0 to 255.

Default 0x80

Format **`lacp actor port priority`** <*priority*>

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format **`no lacp actor port priority`**

Mode Interface Config

lacp actor system priority

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for <*priority*> is 0 to 255.

Default 0x80

Format **`lacp actor system priority`** <*priority*>

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor system priority

Use this command to configure the priority value associated with the Actor's SystemID.

Format **`lacp actor system priority`**

Mode Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. The valid range for <*key*> is 0 to 65535.

Default 0x0

Format **`lacp partner admin key <key>`**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner.

Format **`no lacp partner admin key <key>`**

Mode Interface Config

lacp partner admin state

Use this command to configure the current administrative value of actor state for the protocol Partner. The valid value range is 0x00-0xFF.

Default 0x07

Format **`lacp partner admin state {individual|longtimeout|passive}`**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state

Use this command the configure the default current administrative value of actor state for the protocol partner.

Format **`no lacp partner admin state {individual|longtimeout|passive}`**

Mode Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format **`lacp partner admin state individual`**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format `no lacp partner admin state individual`
Mode Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format `lacp partner admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format `no lacp partner admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format `lacp partner admin state passive`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format `no lacp partner admin state passive`
Mode Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. The valid range for <*port-id*> is 0 to 65535.

Default 0x80
Format `lacp partner port-id <port-id>`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format `lacp partner port-id`
Mode Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. The valid range for <*priority*> is 0 to 255.

Default 0x0
Format `lacp partner port priority <priority>`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format `no lacp partner port priority`
Mode Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. The valid range of <*system-id*> is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default 00:00:00:00:00:00

Format **lacp partner system-id** <*system-id*>

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format **no lacp partner system-id**

Mode Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. The valid range for <*priority*> is 0 to 255.

Default 0x0

Format **lacp partner system priority** <*priority*>

Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format **no lacp partner system priority**

Mode Interface Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in

the system, the static mode for a new port-channel enabled, which means the port-channel is static.You can only use this command on port-channel interfaces.

Default disabled

Format `port-channel static`

Mode Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format `no port-channel static`

Mode Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

Default enabled

Format `port lacpmode`

Mode Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format `no port lacpmode`

Mode Interface Config

port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format `port lacpmode all`

Mode Global Config

no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format `no port lacpmode all`

Mode Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default long

Format **`port lacptimeout`** *{actor | partner} {long | short}*

Mode Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (**actor** or **partner**).

Format **`no port lacptimeout`** *{actor | partner}*

Mode Interface Config

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default long

Format **`port lacptimeout`** *{actor | partner} {long | short}*

Mode Global Config

Default long

Format **`port lacptimeout`** *{actor | partner} {long | short}*

Mode Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (**actor** or **partner**) back to their default values.

Format **`no port lacptimeout`** *{actor | partner}*

Mode Global Config

port-channel adminmode

This command enables a port-channel (LAG). The option **`all`** sets every configured port-channel with the same administrative mode setting.

Format **`port-channel adminmode`** *[all]*

Mode Global Config

no port-channel adminmode

This command disables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Format **no port-channel adminmode** *[all]*

Mode Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Default enabled

Format **port-channel linktrap** *{<logical slot/port> | all}*

Mode Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format **no port-channel linktrap** *{<logical slot/port> | all}*

Mode Global Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

Format **port-channel name** *{<logical slot/port> | all | <name>}*

Mode Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of <priority> is 0-65535.

Default 0x8000

Format **port-channel system priority** <*priority*>

Mode Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format `no port-channel system priority`
Mode Global Config

show lacp actor

Use this command to display LACP actor attributes.

Format `show lacp actor {<slot/port>|all}`
Mode Global Config

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes.

Format `show lacp actor {<slot/port>|all}`
Mode Privileged EXEC

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format `show port-channel brief`

Mode
- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

Term	Definition
Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Type	Shows whether the port-channel is statically or dynamically maintained.
LACP Device Type/Timeout	The timeout (**long** or **short**) for the type of device (**actor** or **partner**).
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format `show port-channel {<logical slot/port> | all}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Logical Interface	Valid slot and port number separated by a forward slash.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

show port-channel system priority

Use this command to display the port-channel system priority.

Format `show port-channel system priority`

Mode Privileged EXEC

PORT MIRRORING

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the *source interface <slot/port>* parameter to specify the interface to monitor. Use *rx* to monitor only ingress packets, or use *tx* to monitor only egress packets. If you do not specify an *{rx | tx}* option, the destination port monitors both ingress and egress packets. Use the *destination interface <slot/port>* to specify the interface to receive the monitored traffic. Use the *mode* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format **monitor session** *<session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> | mode}*

Mode Global Config

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the *source interface <slot/port>* parameter or *destination interface <slot/port>* to remove the specified interface from the port monitoring session. Use the *mode* parameter to disable the administrative mode of the session.

Note: Since the current version of FL SWITCH GHS Firmware software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the **no monitor** command.

Format **no monitor session** *<session-id> [{source interface <slot/port> | destination interface <slot/port> | mode}]*

Mode Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

Note: This is a stand-alone “no” command. This command does not have a “normal” form.

Default enabled

Format **no monitor**

Mode Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

Note: The *<session-id>* parameter is an integer value used to identify the session. In the current version of the software, the *<session-id>* parameter is always one (1).

Format **show monitor session** *<session-id>*

Mode Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <*session-id*>. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with *<session-id>*. If probe port is not set then this field is blank.
Source Port	The port, which is configured as mirrored port (source port) for the session identified with *<session-id>*. If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

IGMP SNOOPING CONFIGURATION COMMANDS

This section describes the commands you use to configure IGMP snooping. FL SWITCH GHS Firmware software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and

discarding of the frame upon checksum error.

- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format **`set igmp`**

Mode
- Global Config
- Interface Config

Format **`set igmp`** *<vlanid>*

Mode VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface or a VLAN.

Format **`no set igmp`**

Mode
- Global Config
- Interface Config

Format **`no set igmp`** *<vlanid>*

Mode VLAN Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default disabled

Format **`set igmp interfacemode`**

Mode Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format **`no set igmp interfacemode`**

Mode Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default disabled

Format **`set igmp fast-leave`**

Mode Interface Config

Format **`set igmp fast-leave`** *<vlan_id>*

Mode VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format **`no set igmp fast-leave`**

Mode Interface Config

Format **`no set igmp fast-leave`** *<vlan_id>*

Mode VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format **`set igmp groupmembership-interval`** *`<2-3600>`*

Mode
- Interface Config
- Global Config

Format **`set igmp groupmembership-interval`** *`<vlan_id> <2-3600>`*

Mode VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format **`no set igmp groupmembership-interval`**

Mode
- Interface Config
- Global Config

Format **`no set igmp groupmembership-interval`** *`<vlan_id>`*

Mode VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, or on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default 10 seconds

Format **`set igmp maxresponse`** *`<1-25>`*

Mode
- Global Config
- Interface Config

Format **`set igmp maxresponse`** *`<vlan_id> <1-25>`*

Mode VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format **no set igmp maxresponse**

Mode
- Global Config
- Interface Config

Format **no set igmp maxresponse** *<vlan_id>*

Mode VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default 0

Format **set igmp mcrtrexpiretime** *<0-3600>*

Mode
- Global Config
- Interface Config

Format **set igmp mcrtrexpiretime** *<vlan_id> <0-3600>*

Mode VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format **no set igmp mcrtrexpiretime**

Mode
- Global Config
- Interface Config

Format **no set igmp mcrtrexpiretime** *<vlan_id>*

Mode VLAN Config

set igmp mrouter

This command configures the VLAN ID (*<vlanId>*) that has the multicast router mode enabled.

Format **set igmp mrouter <***vlan_id***>**

Mode Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (<*vlan_id*>).

Format **no set igmp mrouter <***vlan_id***>**

Mode Interface Config

set igmp mrouter interface

This command configures the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default disabled

Format **set igmp mrouter interface**

Mode Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format **no set igmp mrouter interface**

Mode Interface Config

show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

Format **show igmpsnooping** *[<slot/port> | <vlan_id>]*

Mode Privileged EXEC

When the optional arguments <*slot/port*> or <*vlan_id*> are not used, the command displays the following information:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *<slot/port>* values, the following information appears:

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *<vlan_id>*, the following information appears:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format **`show igmpsnooping mrouter interface`** *<slot/port>*

Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter vlan` *<slot/port>*

Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

Mode Privileged EXEC

Term	Definition
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP SNOOPING QUERIER COMMANDS

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set igmp querier [<vlan-id>] [address ipv4_address]`

Mode
- Global Config
- VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional *address* parameter to reset the querier address to 0.0.0.0.

Format `no set igmp querier [<vlan-id>] [address]`

Mode
- Global Config
- VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format **`set igmp querier query-interval`** *<1-18000>*

Mode Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format **`no set igmp querier query-interval`**

Mode Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format **`set igmp querier timer expiry`** *<60-300>*

Mode Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format `no set igmp querier timer expiry`
Mode Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default 1
Format `set igmp querier version <1-2>`
Mode Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format `no set igmp querier version`
Mode Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled
Format `set igmp querier election participate`
Mode VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format `no set igmp querier election participate`
Mode VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format `show igmpsnooping querier [{detail | vlan <vlanid>}]`

Mode Privileged EXEC

When the optional argument <*vlanid*> is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for <*vlanid*>, the following additional information appears.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

PORT SECURITY COMMANDS

Default

Format

Mode

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note: To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 33.

port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

Default disabled

Format `port-security`

Mode
- Global Config
- Interface Config

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format `no port-security`

Mode
- Global Config
- Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default 600

Format **`port-security max-dynamic`** *<maxvalue>*

Mode Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format `no port-security max-dynamic`

Mode Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default 20

Format `port-security max-static <maxvalue>`

Mode Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format `no port-security max-static`

Mode Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The `<vid>` is the VLAN ID.

Format `port-security mac-address <mac-address> <vid>`

Mode Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format `no port-security mac-address <mac-address> <vid>`

Mode Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Format `port-security mac-address move`

Mode Interface Config

show port-security

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format **show port-security** *[{<slot/port> | all}]*

Mode Privileged EXEC

Term	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Term	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format **show port-security dynamic** *<slot/port>*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port.

Format **show port-security static** *<slot/port>*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of statically locked MAC.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format **`show port-security violation`** *<slot/port>*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of discarded packet on locked port.

LLDP (802.1AB) COMMANDS

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability.

Default disabled

Format **`lldp transmit`**

Mode Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format **`no lldp transmit`**

Mode Interface Config

lldp receive

Use this command to enable the LLDP receive capability.

Default disabled

Format **`lldp receive`**

Mode Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format **no lldp receive**

Mode Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *<interval-seconds>* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *<hold-value>* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *<reinit-seconds>* is the delay before re-initialization, and the range is 1-0 seconds.

Default
- interval—30 seconds
- hold—4
- reinit—2 seconds

Format **lldp timers** *[interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>*]

Mode Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format **no lldp timers** *[interval] [hold] [reinit]*

Mode Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use *sys-name* to transmit the system name TLV. To configure the system name, see See “snmp-server” on page 31. Use *sys-desc*to transmit the system description TLV. Use *sys-cap* to transmit the system capabilities TLV. Use *port-desc* to transmit the port description TLV. To configure the port description, see See “description” on page 2.

Default no optional TLVs are included

Format **lldp transmit-tlv** *[sys-desc] [sys-name] [sys-cap] [port-desc]*

Mode Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs.

Format `lldp transmit-mgmt`

Mode Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format `no lldp transmit-mgmt`

Mode Interface Config

lldp notification

Use this command to enable remote data change notifications.

Default disabled

Format `lldp notification`

Mode Interface Config

no lldp notification

Use this command to disable notifications.

Default disabled

Format `no lldp notification`

Mode Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *<interval>* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default 5

Format **lldp notification-interval** *<interval>*

Mode Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format **no lldp notification-interval**

Mode Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format **clear lldp statistics**

Mode Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format **clear lldp remote-data**

Mode Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format **show lldp**

Mode Privileged Exec

Term	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before re-initialization, in seconds.

Term	Definition
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format **`show lldp interface`** *{<slot/port> | all}*

Mode Privileged Exec

Term	Definition
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format **`show lldp statistics`** *{<slot/port> | all}*

Mode Privileged Exec

Term	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	Definition
Interface	The interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.

Term	Definition
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format **`show lldp remote-device`** *{<slot/port> | all}*

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Chassis ID	The ID of the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format **`show lldp remote-device detail`** *<slot/port>*

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.

Term	Definition
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format **`show lldp local-device`** *{<slot/port> | all}*

Mode Privileged EXEC

Term	Definition
Interface	The interface in a slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format **`show lldp local-device detail`** *<slot/port>*

Mode Privileged EXEC

Term	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.

Term	Definition
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED COMMANDS

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default disabled

Format `lldp med`

Mode Interface Config

no lldp med

Use this command to disable MED.

Format `no lldp med`

Mode Interface Config

lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default disabled

Format `lldp med confignotification`

Mode Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format `no lldp med confignotification`

Mode Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format **`lldp med transmit-tlv`** `[capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Interface Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format **`no lldp med transmit-tlv`** *`[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`*

Mode Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format **`lldp med all`**

Mode Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format **`lldp med confignotification all`**

Mode Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *[count]* is then umber of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format **lldp med faststartrepeatcount** *[count]*

Mode Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format **no lldp med faststartrepeatcount**

Mode Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format **lldp med transmit-tlv all** [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]

Mode Global Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format **no lldp med transmit-tlv** *[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]*

Mode Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format **`show lldp med`**

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(FL SWITCH GHS Firmware Routing) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *<unit/slot/port>* indicates a specific physical interface. *all* indicates all valid LLDP interfaces.

Format **`show lldp med interface`** *{<unit/slot/port> | all}*

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/1      Down    Disabled  Disabled  Disabled     0,1
1/0/2      Up      Disabled  Disabled  Disabled     0,1
1/0/3      Down    Disabled  Disabled  Disabled     0,1
1/0/4      Down    Disabled  Disabled  Disabled     0,1
1/0/5      Down    Disabled  Disabled  Disabled     0,1
1/0/6      Down    Disabled  Disabled  Disabled     0,1
1/0/7      Down    Disabled  Disabled  Disabled     0,1
1/0/8      Down    Disabled  Disabled  Disabled     0,1
1/0/9      Down    Disabled  Disabled  Disabled     0,1
1/0/10     Down    Disabled  Disabled  Disabled     0,1
1/0/11     Down    Disabled  Disabled  Disabled     0,1
1/0/12     Down    Disabled  Disabled  Disabled     0,1
1/0/13     Down    Disabled  Disabled  Disabled     0,1
1/0/14     Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(FL SWITCH GHS Firmware Routing) #show lldp med interface 1/0/2
```

```
Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/2      Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(FL SWITCH GHS Firmware Routing) #
```

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. *<slot/port>* indicates a specific physical interface.

Format **show lldp med local-device detail** *<slot/port>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med local-device detail
1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

Network Policies
Media Policy Application Type: voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type: streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx
```

```
Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format **show lldp med remote-device** *{<slot/port> | all}*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Device Class
---------  -----------------
1/0/8      Class I
1/0/9      Not Defined
1/0/10     Class II
1/0/11     Class III
1/0/12     Network Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format **show lldp med remote-device detail** *<slot/port>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med remote-device detail
1/0/8

Local Interface: 1/0/8

Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location,
extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type: voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type: streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

DENIAL OF SERVICE COMMANDS

Note: Denial of Service (DataPlane) is not supported on the XGSII Tucana Platform. DoS is supported on XGSIII platforms only.

This section describes the commands you use to configure Denial of Service (DoS) Control. FL SWITCH GHS Firmware software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block six types of attacks:

- **SIP=DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control sipdip`

Mode Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP=DIP) Denial of Service prevention.

Format `no dos-control sipdip`

Mode Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if

the mode is enabled.The default is *disabled*. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to *20*.

Default disabled <20>

Format **dos-control firstfrag** [<0-255>]

Mode Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format **no dos-control firstfrag**

Mode Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default disabled

Format **dos-control tcpfrag**

Mode Global Config

no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format **no dos-control tcpfrag**

Mode Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default disabled

Format **dos-control tcpflag**

Mode Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format `no dos-control tcpflag`

Mode Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note: Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default disabled

Format `dos-control l4port`

Mode Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format `no dos-control l4port`

Mode Global Config

dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default disabled <512>

Format `dos-control icmp` *<0-1023>*

Mode Global Config

no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format `no dos-control icmp`

Mode Global Config

show dos-control

This command displays Denial of Service configuration information.

Format `show dos-control`

Mode Privileged EXEC

Term	Definition
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMP Pkt Size <0-1023>	The factory default is 512.

MAC DATABASE COMMANDS

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The *<seconds>* parameter must be within the range of 10 to 1,000,000 seconds.

Default 300

Format `bridge aging-time` *<10-1,000,000>*

Mode Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format `no bridge aging-time`

Mode Global Config

show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

Default all

Format **`show forwardingdb agetime`** *`[fdbid | all]`*

Mode Privileged EXEC

Term	Definition
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.
Agetime	• In an IVL system, this parameter displays the address aging timeout for the associated forwarding database. •

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format **`show mac-address-table multicast`** *`<macaddr>`*

Mode Privileged EXEC

Term	Definition
MAC Address	A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format **`show mac-address-table stats`**

Mode Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

INTERNET GROUP MESSAGE PROTOCOL (IGMP) COMMANDS

This section describes the commands you use to view and configure IGMP settings.

ip igmp

This command sets the administrative mode of IGMP in the system to active.

Default disabled

Format `ip igmp`

Modes
- Global Config
- Interface Config

no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format `no ip igmp`

Modes
- Global Config
- Interface Config

ip igmp version

This command configures the version of IGMP for an interface. The value for *<version>* is either 1, 2 or 3.

Default 3

Format `ip igmp version <version>`

Modes Interface Config

no ip igmp version

This command resets the version of IGMP to the default value.

Format `no ip igmp version`

Modes Interface Config

ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface. The range for *<count>* is 1 to 20.

Format `ip igmp last-member-query-count <count>`

Modes Interface Config

no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format `no ip igmp last-member-query-count`

Modes Interface Config

ip igmp last-member-query-interval

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for <*seconds*> is 0 to 255 tenths of a second.

Default 10 tenths of a second (1 second)

Format `ip igmp last-member-query-interval <`*seconds*`>`

Modes Interface Config

no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format `no ip igmp last-member-query-interval`

Modes Interface Config

ip igmp query-interval

This command configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for <*queryinterval*> is 1 to 3600 seconds.

Default 125 seconds

Format `ip igmp query-interval <`*seconds*`>`

Modes Interface Config

no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format `no ip igmp query-interval`

Modes Interface Config

ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this

interface.The time interval is specified in tenths of a second. The range for <*maxresptime*> is 0 to 255 tenths of a second.

Default 100

Format **ip igmp query-max-response-time <*seconds*>**

Mode Interface Config

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format **no ip igmp query-max-response-time**

Mode Interface Config

ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for <*robustness*> is 1 to 255.

Default 2

Format **ip igmp robustness <*robustness*>**

Mode Interface Config

no ip igmp robustness

This command sets the robustness value to default.

Format **no ip igmp robustness**

Mode Interface Config

ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface. The range for <*count*> is 1 to 20.

Default 2

Format **ip igmp startup-query-count <*count*>**

Mode Interface Config

no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format `no ip igmp startup-query-count`

Mode Interface Config

ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds. The range for *<interval>* is 1 to 300 seconds.

Default 31

Format `ip igmp startup-query-interval <interval>`

Mode Interface Config

no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format `no ip igmp startup-query-interval`

Mode Interface Config

show ip igmp

This command displays the system-wide IGMP information.

Format `show ip igmp`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	Valid slot and port number separated by a forward slash.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

show ip igmp groups

This command displays the registered multicast groups on the interface. If *[detail]* is specified this command displays the registered multicast groups on the interface in detail.

Format `show ip igmp groups <slot/port> [detail]`

Mode Privileged EXEC

If you do not use the **detail** keyword, the following fields appear:

Term	Definition
IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	The subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Term	Definition
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If you use the **detail** keyword, the following fields appear:

Term	Definition
Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

show ip igmp interface

This command displays the IGMP information for the interface.

Format **show ip igmp interface** <*slot/port*>

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Term	Definition
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.
Query Max Response Time	The maximum query response time advertised in IGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format **`show ip igmp interface membership`** *<multiipaddr> [detail]*

Mode Privileged EXEC

Term	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If you use the **`detail`** keyword, the following fields appear:

Term	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format `show ip igmp interface stats` *<slot/port>*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	The IP address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface.

IGMP PROXY COMMANDS

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

ip igmp-proxy

This command enables the IGMP Proxy on the router. To enable the IGMP Proxy on the router, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

Format `ip igmp-proxy`

Mode Interface Config

no ip igmp-proxy

This command disables the IGMP Proxy on the router.

Format `no ip igmp-proxy`

Mode Interface Config

ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface. The value of *<interval>* can be 1-260 seconds.

Default 1

Format **ip igmp-proxy unsolicit-rprt-interval** *<interval>*

Mode Interface Config

no ip igmp-proxy unsolicit-rprt-interval

This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format **no ip igmp-proxy unsolicit-rprt-interval**

Mode Interface Config

ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface.

Format **ip igmp-proxy reset-status**

Mode Interface Config

show ip igmp-proxy

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format **show ip igmp-proxy**

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or not. This is a configured value.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).

Term	Definition
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format `show ip igmp-proxy interface`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Index	The slot/port of the IGMP proxy.

The column headings of the table associated with the interface are as follows:

Term	Definition
Ver	The IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received.
Leaves Sent	Number of IGMP leaves sent.

show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format `show ip igmp-proxy groups`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report.
Up Time (in secs)	The time elapsed since last created.

Term	Definition
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER - interface has responded to the latest group membership query for this group. • DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format `show ip igmp-proxy groups detail`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. IDLE_MEMBER - interface has responded to the latest group membership query for this group. DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are include or exclude.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

STATIC MCAST CONFIGURATION

This command is creating or deleting a static multicast group.

Static_mcast create

Default disable

Format `config Set Static_mcast create <mac_addr>`

Mode Privileged EXEC

Static_mcast delete

Default disable

Format `config Set Static_mcast delete <mac_addr>`

Mode Privileged EXEC

This command is adding or removing ports to or from a group.

add_port

Default disable

Format `interface Set Static_mcast add_port <mac_addr>`

Mode Privileged EXEC

rem_port

Default disable

Format `interface Set Static_mcast rem_port <mac_addr>`

Mode Privileged EXEC

SET IGMP

This command is defining if a unknown multicast will be forwarded to a querier.

block-unknown-mcast

Default disable

Format `config Set IGMP block-unknown-mcast`

Mode Privileged EXEC

forward-unknown-mcast

Default enable

Format `config Set IGMP forward-unknown-mcast`

Mode Privileged EXEC

Section 3: Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the FL SWITCH GHS Firmware CLI.

Note: The commands in this chapter are in one of two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

CLASS OF SERVICE (COS) COMMANDS

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *<userpriority>* values can range from 0-7. The *<trafficclass>* values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see "Voice VLAN Commands" on page 47.

Format `classofservice dot1p-mapping` *<userpriority> <trafficclass>*

Modes
- Global Config
- Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format `no classofservice dot1p-mapping`

Modes
- Global Config
- Interface Config

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *<ipdscp>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The *<trafficclass>* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format **`classofservice ip-dscp-mapping`** *<ipdscp> <trafficclass>*

Mode Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format **`no classofservice ip-dscp-mapping`**

Mode Global Config

classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the **`show running config`** command because Dot1p is the default.

Note: The **classofservice trust dot1p** command will not be supported in future releases of the software because Dot1p is the default value. Use the **no classofservice trust** command to set the mode to the default value.

Default dot1p

Format **`classofservice trust`** *{dot1p | ip-dscp | ip-precedence | untrusted}*

Modes
- Global Config
- Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format **`no classofservice trust`**

Modes
- Global Config
- Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format **cos-queue min-bandwidth** *<bw-0> <bw-1> … <bw-n>*

Modes
- Global Config
- Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format **no cos-queue min-bandwidth**

Modes
- Global Config
- Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

Format **cos-queue strict** *<queue-id-1> [<queue-id-2> … <queue-id-n>]*

Modes
- Global Config
- Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format **no cos-queue strict** *<queue-id-1> [<queue-id-2> … <queue-id-n>]*

Modes
- Global Config
- Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format **traffic-shape** *<bw>*

Modes
- Global Config
- Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes
- Global Config
- Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The *<slot/port>* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see "Voice VLAN Commands" on page 47.

Format `show classofservice dot1p-mapping` *[<slot/port>]*

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice ip-precedence-mapping` *[<slot/port>]*

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format `show classofservice ip-dscp-mapping`

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. The *<slot/port>* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format `show classofservice trust` *[<slot/port>]*

Mode Privileged EXEC

Term	Definition
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show interfaces cos-queue` *[<slot/port>]*

Mode Privileged EXEC

Term	Definition
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.

Term	Definition
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	Definition
Interface	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

MAC ACCESS CONTROL LIST (ACL) COMMANDS

This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *<name>*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *<name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format **`mac access-list extended`** *<name>*

Mode Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *<name>* from the system.

Format **no mac access-list extended** *<name>*

Mode Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *<name>* parameter is the name of an existing MAC ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *<newname>* already exists.

Format **mac access-list extended rename** *<name> <newname>*

Mode Global Config

{deny | permit}

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note: An implicit 'deny all' MAC rule always terminates the access list.

Note: For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *<ethertypekey>* values are: appletalk, arp,

ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 9: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a **permit** rule.

For the device, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.

Note: The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

Note: The special command form **{deny | permit} any any** is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

Format *{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]] [{mirror | redirect} <slot/port>]*

Mode Mac-Access-List Config

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface, or associates it with a VLAN ID, in a given direction. The *<name>* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Format **mac access-group** *<name> [vlan <vlan-id>]* **in** *[sequence <1-4294967295>]*

Modes
- Global Config
- Interface Config

no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format **no mac access-group** *<name> [vlan <vlan-id>]* **in**

Modes
- Global Config
- Interface Config

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the *[name]* parameter to identify a specific MAC ACL to display.

Format **show mac access-lists** *[name]*

Mode Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.

Term	Definition
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	On this device, the slot/port to which packets matching this rule are forwarded.

IP Access Control List (ACL) Commands

This section describes the commands you use to configure IP ACL settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- FL SWITCH GHS Firmware software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On Broadcom 5630x platforms, if you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0’s) in a bit position that must be checked. A ‘1’ in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 10 describes the parameters for the **`access-list`** command.

IP Standard ACL:

Format **`access-list`** *<1-99> {deny | permit} {every | <srcip> <srcmask>} [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]*

Mode Global Config

IP Extended ACL:

Format **access-list** *<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]*

Mode Global Config

Table 10: ACL Command Parameters

Parameter	Description
<1-99> or *<100-199>*	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. ***Note:*** For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet
{icmp | igmp | ip | tcp | udp | <number>}	Specifies the protocol to filter for an extended IP ACL rule.
<srcip> <srcmask>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
[{eq {<portkey> | <0-65535>}]	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *<portkey>*, which can be one of the following keywords: *domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp*, and *www*. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<dstip> <dstmask>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos/tosmask*.
[log]	Specifies that this rule is to be logged.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[{mirror | redirect} <slot/port>]	For this device, specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively. The *mirror* and *redirect* parameters are not available on this device.

no access-list

This command deletes an IP ACL that is identified by the parameter *<accesslistnumber>* from the system. The range for *<accesslistnumber>* 1-99 for standard access lists and 100-199 for extended access lists.

Format **no access-list** *<accesslistnumber>*

Mode Global Config

ip access-group

This command either attaches a specific IP ACL identified by *<accesslistnumber>* to an interface or associates with a VLAN ID in a given direction.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default none

Format **ip access-group** *<accesslistnumber> [vlan <vlan-id>]* **in** *[sequence <1-4294967295>]*

Modes
- Interface Config
- Global Config

no ip access-group

This command removes a specified IP ACL from an interface.

Default none

Format **no ip access-group** *<accesslistnumber> [vlan <vlan-id>]* **in**

Mode
- Interface Config
- Global Config

acl-trapflags

This command enables the ACL trap mode.

Default disabled

Format **acl-trapflags**

Mode Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format **no acl-trapflags**

Mode Global Config

show ip access-lists

This command displays an IP ACL *<accesslistnumber>* is the number used to identify the IP ACL.

Format **show ip access-lists** *<accesslistnumber>*

Mode Privileged EXEC

Note: Only the access list fields that you configure are displayed.

Term	Definition
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

Format **show access-lists interface** *<slot/port>* **in**

Mode Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).

Term	Definition
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

Section 4: Utility Commands

This chapter describes the utility commands available in the FL SWITCH GHS Firmware CLI.

Note: The commands in this chapter are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

Dual Image Commands

FL SWITCH GHS Firmware software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays.

Format `delete {image1 | image2}`

Mode Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots.

Format `boot system <image-file-name>`

Mode Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format `show bootvar`

Mode Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format `filedescr {image1 | image2} <text-description>`

Mode Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

Format `update bootcode`

Mode Privileged EXEC

SYSTEM INFORMATION AND STATISTICS COMMANDS

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format `show arp switch`

Mode Privileged EXEC

Term	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is *Management*. For a network port, the output is the slot/port of the physical interface.

show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format `show eventlog`

Mode Privileged EXEC

Term	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

Note: Event log information is retained across a switch reset.

show hardware

This command displays inventory information for the switch.

Note: The **show version** command and the **show hardware** command display the same information. In future releases of the software, the **show hardware** command will not be available. For a description of the command output, see the command "show version" on page 3.

Format `show hardware`

Mode Privileged EXEC

show version

This command displays inventory information for the switch.

Note: The **show version** command will replace the **show hardware** command in future releases of the software.

Format `show version`

Mode Privileged EXEC

Term	Definition
Switch Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.

Term	Definition
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format **show interface** *{<slot/port> | switchport}*

Mode Privileged EXEC

The display parameters, when the argument is *<slot/port>*, are as follows:

Parameters	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” are as follows:

Term	Definition
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Term	Definition
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format **`show interface ethernet`** *{<slot/port> | switchport}*

Mode Privileged EXEC

When you specify a value for *<slot/port>*, the command displays the following information.

Term	Definition
Packets Received	• **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. • **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received > 1522 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1519–1522 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1523–2047 Octets** - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Term	Definition
Packets Received Successfully	• **Total Packets Received Without Error** - The total number of packets received that were without errors. • **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	• **Total** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	• **Total** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process • **Local Traffic Frames** - The total number of frames dropped in the forwarding process because the destination address was located off of this port. • **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type. • **Multicast Tree Viable Discards** - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified. • **Reserved Address Discards** - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system. • **Broadcast Storm Recovery** - The number of frames discarded that are destined for `FF:FF:FF:FF:FF:FF` when Broadcast Storm Recovery is enabled. • **CFI Discards** - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format. • **Upstream Threshold** - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Term	Definition
Packets Transmitted Octets	• **Total Bytes** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- • **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit.
Packets Transmitted Successfully	• **Total** - The number of frames that have been transmitted by this port to its segment. • **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. • **Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. • **Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Errors	• **Total Errors** - The sum of Single, Multiple, and Excessive Collisions. • **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. • **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
Transmit Discards	• **Total Discards** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded. • **Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. • **Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. • **Excessive Collisions** - A count of frames for which transmission on a particular interface fails due to excessive collisions. • **Port Membership Discards** - The number of frames discarded on egress for this port due to egress filtering being enabled.

Term	Definition
Protocol Statistics	• **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **GVRP PDUs Received** - The count of GVRP PDUs received in the GARP layer. • **GVRP PDUs Transmitted** - The count of GVRP PDUs transmitted from the GARP layer. • **GVRP Failed Registrations** - The number of times attempted GVRP registrations could not be completed. • **GMRP PDUs Received** - The count of GMRP PDU's received in the GARP layer. • **GMRP PDUs Transmitted** - The count of GMRP PDU's transmitted from the GARP layer. • **GMRP Failed Registrations** - The number of times attempted GMRP registrations could not be completed. • **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. • **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	• **EAPOL Frames Received** - The number of valid EAPOL frames of any type that have been received by this authenticator. • **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the *switchport* keyword, the following information appears.

Term	Definition
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Total Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.

Term	Definition
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter *all* or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the *count* parameter to view summary information about the forwarding database table. Use the *interface <slot/port>* parameter to view MAC addresses on a specific interface. Use the *vlan <vlan_id>* parameter to display information about MAC addresses on a specified VLAN.

Format **show mac-addr-table** *[{<macaddr> <vlan_id> | all | count | interface <slot/port> | vlan <vlan_id>}]*

Mode Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID. If you enter *vlan <vlan_id>*, only the Mac Address, Interface, and Status fields appear.

Term	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example `01:23:45:67:89:AB`. In an IVL system the MAC address will be displayed as 8 bytes.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • *Static*—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • *Learned*—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • *Management*—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • *Self*—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). • *GMRP Learned*—The value of the corresponding was learned via GMRP and applies to Multicast. • *Other*—The value of the corresponding instance does not fall into one of the other categories.

If you enter the *interface <slot/port>* parameter, in addition to the MAC Address and Status fields, the following field appears:

Term	Definition
VLAN ID	The VLAN on which the MAC address was learned.

The following information displays if you enter the *count* parameter:

Term	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the *[all]* option.

Note: Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *<scriptname>* is provided with a file name extension of ".scr", the output is redirected to a script file.

Note: If you issue the **show running-config** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Note: If you use a text-based configuration file, the **show running-config** command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the **show running-config** command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its 'exit' command, are both omitted from the **show running-config** command output (and hence from the startup-config file when the system configuration is saved.)

This command captures the current settings of OSPFv2 and OSPFv3 trapflag status:

- If all the flags are enabled, then the command displays **trapflags all**.
- If all the flags in a particular group are enabled, then the command displays **trapflags** *<group name>* **all**.
- If some, but not all, of the flags in that group are enabled, the command displays **trapflags** *<groupname> <flag-name>.*

Format **show running-config** *[all | <scriptname>]*

Mode Privileged EXEC

show sysinfo

This command displays switch information.

Format **show sysinfo**

Mode Privileged EXEC

Term	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see "snmp-server" on page 31.

Term	Definition
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see “snmp-server” on page 31.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see “snmp-server” on page 31.
System ObjectID	The base object ID for the switch’s enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the **`show tech-support`** command to display system and configuration information when you contact technical support. The output of the **`show tech-support`** command combines the output of the following commands:

- **`show version`**
- **`show sysinfo`**
- **`show port all`**
- **`show logging`**
- **`show event log`**
- **`show logging buffered`**
- **`show trap log`**
- **`show running config`**

Format **`show tech-support`**

Mode Privileged EXEC

terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the **`show running-config`** and **`show running-config all`** commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More-- or (q)uit`. Press `q` or `Q` to quit, or press any key to display the next set of <*5-48*> lines. The command **`terminal length 0`** disables pagination and, as a result, the output of the **`show running-config`** command is displayed immediately.

Default 24 lines per page

Format **`terminal length`** <`0`|*5-48*>

Mode Privileged EXEC

no terminal length

Use this command to set the terminal length to the default value.

show terminal length

Use this command to display the value of the user-configured terminal length size.

Format `show terminal length`
Mode Privileged EXEC

LOGGING COMMANDS

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default disabled; critical when enabled
Format `logging buffered`
Mode Global Config

no logging buffered

This command disables logging to in-memory log.

Format `no logging buffered`
Mode Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default enabled
Format `logging buffered wrap`
Mode Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format `no logging buffered wrap`
Mode Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the FL SWITCH GHS Firmware software to log all CLI commands issued on the system.

Default enabled

Format **`logging cli-command`**

Mode Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format **`no logging cli-command`**

Mode Global Config

logging console

This command enables logging to the console. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **`emergency`** (0), **`alert`** (1), **`critical`** (2), **`error`** (3), **`warning`** (4), **`notice`** (5), **`info`** (6), or **`debug`** (7).

Default disabled; critical when enabled

Format **`logging console`** *[severitylevel]*

Mode Global Config

no logging console

This command disables logging to the console.

Format **`no logging console`**

Mode Global Config

logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr|hostname>* is the IP address of the logging host. The *<addresstype>* indicates the type of address ipv4 or ipv6 or dns being passed. The *<port>* value is a port number from 1 to 65535. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **`emergency`** (0), **`alert`** (1), **`critical`** (2), **`error`** (3), **`warning`** (4), **`notice`** (5), **`info`** (6), or **`debug`** (7).

Default
- port—514
- level—critical (2)

Format **`logging host`** *<ipaddr|hostname> <addresstype> [<port>][<severitylevel>]*

Mode Global Config

logging host remove

This command disables logging to host. See "show logging hosts" on page 18 for a list of host indexes.

Format `logging host remove <hostindex>`
Mode Global Config

logging port

This command sets the local port number of the LOG client for logging messages. The `<portid>` can be in the range from 1 to 65535.

Default 514
Format `logging port <portid>`
Mode Global Config

no logging port

This command resets the local logging port to the default.

Format `no logging port`
Mode Global Config

logging syslog

This command enables syslog logging. The `<portid>` parameter is an integer with a range of 1-65535.

Default disabled
Format `logging syslog [port <portid>]`
Mode Global Config

no logging syslog

This command disables syslog logging.

Format `no logging syslog`
Mode Global Config

show logging

This command displays logging configuration information.

Format `show logging`
Mode Privileged EXEC

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Term	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts.

Format `show logging hosts`

Mode Privileged EXEC

Term	Definition
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.

Term	Definition
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Term	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the **traceroute** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Default

- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop
-

Format

traceroute <*ipaddr*|*hostname*> [**initTtl** <*initTtl*>] [**maxTtl** <*maxTtl*>] [**maxFail** <*maxFail*>] [**interval** <*interval*>] [**count** <*count*>] [**port** <*port*>] [**size** <*size*>]

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
ipaddr|**hostname**	The *ipaddr* value should be a valid IP address. The *hostname* value should be a valid hostname.
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use maxTtle to specify the maximum TTL. Range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use interval to specify the time between probes, in seconds. Range is 1 to 60 seconds.
count	Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional port parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Example: The following are examples of the CLI command.

Example: traceroute Success:

```
(FL SWITCH GHS Firmware Routing) # traceroute 10.240.10.115 initTtl
1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute Failure:

```
(FL SWITCH GHS Firmware Routing) # traceroute 10.40.1.1 initTtl 1
maxFail 0 interval 1 count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter y, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format **`clear config`**

Mode Privileged EXEC

clear counters

This command clears the statistics for a specified *<slot/port>,* for all the ports, or for the entire switch based upon the argument.

Format **`clear counters`** *{<slot/port> | all}*

Mode Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format **`clear igmpsnooping`**

Mode Privileged EXEC

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format **`clear pass`**

Mode Privileged EXEC

clear port-channel

This command clears all port-channels (LAGs).

Format `clear port-channel`
Mode Privileged EXEC

clear traplog

This command clears the trap log.

Format `clear traplog`
Mode Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format `clear vlan`
Mode Privileged EXEC

enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

Format `enable passwd`
Mode Privileged EXEC

enable passwd encrypted *<password>*

This command allows the administrator to transfer the enable password between devices without having to know the password. The *<password>* parameter must be exactly 128 hexidecimal characters.

Format `enable passwd encrypted` *<password>*
Mode Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format `logout`

Modes
- Privileged EXEC
- User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format **ping** *<ipaddress|hostname>* **[count** *<count>***] [interval** *<interval>***] [size** *<size>***]**

Modes
- Privileged EXEC
- User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
count	Use the **count** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *<ip-address>* field. The range for *<count>* is 1 to 15 requests.
interval	Use the **interval** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the **size** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Example: The following are examples of the CLI command.

Example: ping success:

```
(FL SWITCH GHS Firmware Routing) #ping 10.254.2.160 count 3 interval
1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time= 275268 usec
Received response for icmp_seq = 1. time= 274009 usec
Received response for icmp_seq = 2. time= 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: ping failure:

In Case of Unreachable Destination:

```
(FL SWITCH GHS Firmware Routing) # ping 192.168.254.222 count 3
```

```
interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(FL SWITCH GHS Firmware Routing) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format `quit`

Modes
- Privileged EXEC
- User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format `reload`

Mode Privileged EXEC

copy

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

Format **copy** *<source> <destination>*

Mode Privileged EXEC

Replace the *<source>* and *<destination>* parameters with the options in Table 11. For the *<url>* source or destination, use one of the following values:

{xmodem |
tftp://<ipaddr|hostname>|<ip6address>/<filepath>/<filename>
|
sftp|scp://<username>@<ipaddr>|<ipv6address>|<filepath>|<filename>
}

For TFTP, SFTP and SCP, the *<ipaddr|hostname>* parameter is the IP address or host name of the server, *<filepath>* is the path to the file, and *<filename>* is the name of the file you want to upload or download. For SFTP and SCP, the <username> parameter is the username for logging into the remote server via SSH.

Note: *<ip6address>* is also a valid parameter for routing packages that support IPv6.

Caution! Remember to upload the existing FL SWITCH GHS Firmware.cfg file off the switch prior to loading a new release image in order to make a backup.

Table 11: Copy Parameters

Source	Destination	Description
nvram:backup-config	*nvram:startup-config*	Copies the backup configuration to the startup configuration.
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:FL SWITCH GHS Firmware.cfg	*<url>*	Uploads the binary config file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:script <scriptname>	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*nvram:backup-config*	Copies the startup configuration to the backup configuration.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:traplog	*<url>*	Copies the trap log file to a server.
system:running-config	*nvram:startup-config*	Saves the running configuration to nvram.
<url>	*nvram:clibanner*	Downloads the CLI banner to the system.
<url>	*nvram:FL SWITCH GHS Firmware.cfg*	Downloads the binary config file to the system.
<url>	*nvram:script <destfilename>*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
<url>	*nvram:sshkey-dsa*	Downloads an SSH key file. For more information, see “Secure Shell (SSH) Commands” on page 11.
<url>	*nvram:sshkey-rsa1*	Downloads an SSH key file.
<url>	*nvram:sshkey-rsa2*	Downloads an SSH key file.
<url>	*nvram:sslpem-dhweak*	Downloads an HTTP secure-server certificate.
<url>	*nvram:sslpem-dhstrong*	Downloads an HTTP secure-server certificate.

Table 11: Copy Parameters (Cont.)

Source	Destination	Description
<url>	*nvram:sslpem-root*	Downloads an HTTP secure-server certificate. For more information, see "Hypertext Transfer Protocol (HTTP) Commands" on page 15.
<url>	*nvram:sslpem-server*	Downloads an HTTP secure-server certificate.
<url>	*nvram:startup-config*	Downloads the startup configuration file to the system.
<url>	*nvram:system-image*	Downloads a code image to the system.
<url>	*kernel*	Downloads a code file by xmodem, zmodem, or TFTP.
<url>	*{image1 | image2}*	Download an image from the remote server to either image.
{image1 | image2}	*<url>*	Upload either image to the remote server.
image1	*image2*	Copy **image1** to **image2**.
image2	*image1*	Copy **image2** to **image1**.

SIMPLE NETWORK TIME PROTOCOL (SNTP) COMMANDS

This section describes the commands you use to automatically configure the system time and date by using SNTP.

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

Default 6

Format **sntp broadcast client poll-interval** *<poll-interval>*

Mode Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format **no sntp broadcast client poll-interval**

Mode Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default disabled

Format **sntp client mode** *[broadcast | unicast]*

Mode Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format `no sntp client mode`
Mode Global Config

sntp client port

This command sets the SNTP client port id to a value from 1-65535.

Default 123
Format `sntp client port <portid>`
Mode Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format `no sntp client port`
Mode Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where `<poll-interval>` can be a value from 6 to 16.

Default 6
Format `sntp unicast client poll-interval <poll-interval>`
Mode Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-interval`
Mode Global Config

sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default 5
Format `sntp unicast client poll-timeout <poll-timeout>`
Mode Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-timeout`
Mode Global Config

sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default 1
Format `sntp unicast client poll-retry <poll-retry>`
Mode Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-retry`
Mode Global Config

sntp multicast client poll-interval

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

Default 6
Format `sntp multicast client poll-interval <poll-interval>`
Mode Global Config

no sntp multicast client poll-interval

This command resets the poll interval for SNTP multicast clients to its default value.

Format `no sntp multicast client poll-interval`
Mode Global Config

sntp server

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format `sntp server <ipaddress|hostname> [<priority> [<version> [<portid>]]]`
Mode Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove <ipaddress|hostname>`

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Format `show sntp`

Mode Privileged EXEC

Term	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
Multicast Count	Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Term	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`

Mode Privileged EXEC

Term	Definition
Server IP Address / Hostname	IP address or hostname of configured SNTP Server.
Server Type	Address Type of Server.
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server.
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

Section 5: Management Commands

This chapter describes the management commands available in the FL SWITCH GHS Firmware CLI.

Network Interface Commands

Caution! The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see “network mgmt_vlan” on page 20

enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format `enable`

Mode User EXEC

serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

Format `serviceport ip` *<ipaddr> <netmask> [gateway]*

Mode Privileged EXEC

serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Format `serviceport protocol` *{none | bootp | dhcp}*

Mode Privileged EXEC

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

Format **network parms** *<ipaddr> <netmask> [<gateway>]*

Mode Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Default none

Format **network protocol** *{none | bootp | dhcp}*

Mode Privileged EXEC

network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format **network mac-address** *<macaddr>*

Mode Privileged EXEC

network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default burnedin

Format **network mac-type** *{local | burnedin}*

Mode Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format `no network mac-type`

Mode Privileged EXEC

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

Default enabled

Format `network javamode`

Mode Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

Format `no network javamode`

Mode Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format `show network`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.

Term	Definition
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Network Configuration Protocol Current	The network protocol being used. The options are bootp | dhcp | none.
Java Mode	Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is enabled. In FL SWITCH GHS Firmware 4.4.4 and later versions, use the **`show ip http`** command to view this field.
Web Mode	Specifies if the switch should allow access to the Web Interface. The factory default is enabled. In FL SWITCH GHS Firmware 4.4.4 and later versions, use the **`show ip http`** command to view this field.

Example: The following shows example CLI display output for the network port.

```
(admin) #show network

IP Address..................................... 10.250.3.1
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.250.3.3
IPv6 Administrative Mode....................... Enabled
IPv6 Address/Length is .......................
FE80::210:18FF:FE82:337/64
IPv6 Address/Length is ....................... 3099::1/64
IPv6 Address/Length is .......................
3099::210:18FF:FE82:337/64
IPv6 Default Router is .......................
FE80::204:76FF:FE73:423A
Burned In MAC Address.......................... 00:10:18:82:03:37
Locally Administered MAC Address............... 00:00:00:00:00:00
MAC Address Type............................... Burned In
Network Configuration Protocol Current......... None
Management VLAN ID............................. 1
Web Mode....................................... Enable
Java Mode...................................... Enable
```

show serviceport

This command displays service port configuration information.

Format **`show serviceport`**

Mode Privileged EXEC

Term	Definition
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Address/Length	The IPv6 address and length. Default is Link Local format.
IPv6 Default Router	The default gateway address on the service port. The factory default value is an unspecified address.
ServPort Configuration Protocol Current	The network protocol used on the last, or current, power-up cycle, if any.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.

Example: The following shows example CLI display output for the service port.

```
(admin) #show serviceport

IP Address..................................... 10.230.3.51
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.230.3.1
IPv6 Administrative Mode ...................... Enabled
IPv6 Address/Length is .......................
FE80::210:18FF:FE82:338/64
IPv6 Address/Length is ....................... 3017::1/64
IPv6 Address/Length is .......................
3017::210:18FF:FE82:338/64
IPv6 Address/Length is .......................
3024::210:18FF:FE82:338/64
IPv6 Default Router is .......................
FE80::204:76FF:FE73:423A
ServPort Configured Protocol Current........... None
Burned In MAC Address.......................... 00:10:18:82:03:38
```

CONSOLE PORT ACCESS COMMANDS

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format `configuration`

Mode Privileged EXEC

lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

Format `lineconfig`

Mode Global Config

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600

Format `serial baudrate` *{1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}*

Mode Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default 5

Format `serial timeout` *<0-160>*

Mode Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

TELNET COMMANDS

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default enabled

Format `ip telnet server enable`

Mode Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format `no ip telnet server enable`

Mode Privileged EXEC

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *[debug]* is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as 'linemode' where, by default, the operational mode is 'character mode'. The *noecho* option disables local echo.

Format **telnet** *<ip-address|> <port> [debug] [line] [noecho]*

Modes
- Privileged EXEC
- User EXEC

transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the **ip telnet server enable** command to enable Telnet Server Admin Mode.

Default enabled

Format **transport input telnet**

Mode Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format **no transport input telnet**

Mode Line Config

transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default enabled

Format **transport output telnet**

Mode Line Config

no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format `no transport output telnet`

Mode Line Config

session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default 5

Format `session-limit <0-5>`

Mode Line Config

no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format `no session-limit`

Mode Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default 5

Format `session-timeout <1-160>`

Mode Line Config

no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format `no session-timeout`

Mode Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default 5

Format **`telnetcon maxsessions`** *`<0-5>`*

Mode Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format **`no telnetcon maxsessions`**

Mode Privileged EXEC

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Note: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default 5

Format **`telnetcon timeout`** *`<1-160>`*

Mode Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format **`no telnetcon timeout`**

Mode Privileged EXEC

show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format `show telnet`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format `show telnetcon`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

SECURE SHELL (SSH) COMMANDS

This section describes the commands you use to configure SSH access to the switch. Use SSH to access the switch from a remote management host.

Note: The system allows a maximum of 5 SSH sessions.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the **`ip ssh server enable`** command.)

Default disabled

Format **`ip ssh`**

Mode Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default 1 and 2

Format **`ip ssh protocol`** *`[1] [2]`*

Mode Privileged EXEC

ip ssh server enable

This command enables the IP secure shell server.

Default disabled

Format **`ip ssh server enable`**

Mode Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format **`no ip ssh server enable`**

Mode Privileged EXEC

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default 5

Format **`sshcon maxsessions`** *`<0-5>`*

Mode Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format `no sshcon maxsessions`

Mode Privileged EXEC

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default 5

Format `sshcon timeout <1-160>`

Mode Privileged EXEC

no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format `no sshcon timeout`

Mode Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format `show ip ssh`

Mode Privileged EXEC

Term	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.

Term	Definition
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

MANAGEMENT SECURITY COMMANDS

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

crypto certificate generate

Use this command to generate self-signed certificate for HTTPS. The generate RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format `crypto certificate generate`

Mode Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format `no crypto certificate generate`

Mode Global Config

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format `crypto key generate rsa`

Mode Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format `no crypto key generate rsa`

Mode Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format `crypto key generate dsa`
Mode Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format `no crypto key generate dsa`
Mode Global Config

HYPERTEXT TRANSFER PROTOCOL (HTTP) COMMANDS

This section describes the commands you use to configure HTTP and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default enabled
Format `ip http server`
Mode Privileged EXEC

no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format `no ip http server`
Mode Privileged EXEC

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default disabled

Format `ip http secure-server`
Mode Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format `no ip http secure-server`
Mode Privileged EXEC

ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default Enabled
Format `ip http java`
Mode Privileged EXEC

no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format `no ip http java`
Mode Privileged EXEC

ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default 24
Format `ip http session hard-timeout` *<0-168>*
Mode Privileged EXEC

no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format `no ip http session hard-timeout`
Mode Privileged EXEC

ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default 16

Format **ip http session maxsessions** *<0-16>*

Mode Privileged EXEC

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format **no ip http session maxsessions**

Mode Privileged EXEC

ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default 5

Format **ip http session soft-timeout** *<0-60>*

Mode Privileged EXEC

no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format **no ip http session soft-timeout**

Mode Privileged EXEC

ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default 24

Format **ip http secure-session hard-timeout** *<1-168>*

Mode Privileged EXEC

no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format `no ip http secure-session hard-timeout`

Mode Privileged EXEC

ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default 16

Format `ip http secure-session maxsessions` *<0-16>*

Mode Privileged EXEC

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format `no ip http secure-session maxsessions`

Mode Privileged EXEC

ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default 5

Format `ip http secure-session soft-timeout` *<1-60>*

Mode Privileged EXEC

no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format `no ip http secure-session soft-timeout`

Mode Privileged EXEC

ip http secure-port

This command is used to set the SSL port where port can be 1-65535 and the default is port 443.

Default 443

Format `ip http secure-port <portid>`

Mode Privileged EXEC

no ip http secure-port

This command is used to reset the SSL port to the default value.

Format `no ip http secure-port`

Mode Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default SSL3 and TLS1

Format `ip http secure-protocol [SSL3] [TLS1]`

Mode Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format `show ip http`

Mode Privileged EXEC

Term	Definition
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.

Term	Definition
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

ACCESS COMMANDS

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

Use the **`disconnect`** command to close HTTP, HTTPS, Telnet or SSH sessions. Use *`all`* to close all active sessions, or use *`<session-id>`* to specify the session ID to close. To view the possible values for *`<session-id>`*, use the **`show loginsession`** command.

Format **`disconnect`** *`{<session_id> | all}`*

Mode Privileged EXEC

show loginsession

This command displays current Telnet and serial port connections to the switch.

Format **`show loginsession`**

Mode Privileged EXEC

Term	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

USER ACCOUNT COMMANDS

This section describes the commands you use to add, manage, and delete system users. FL SWITCH GHS Firmware software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

users name

This command adds a new user account, if space permits. The account *<username>* can be up to eight characters in length. You can use alphanumeric characters as well as the dash ('-') and underscore ('_'). You can define up to six user names.

Note: The *<username>* is not case sensitive when you add and delete users, and when the user logs in. However, when you use the *<username>* to set the user password, authentication, or encryption, you must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **`show users`** command.

Format **`users name`** *<username>*

Mode Global Config

no users name

This command removes a user account.

Format **`no users name`** *<username>*

Mode Global Config

Note: You cannot delete the "admin" user account.

users name *<username>* unlock

Use this command to unlock a locked user account. Only a user with read/write access can re-activate a locked user account.

Format **`users name`** *<username>* **`unlock`**

Mode Global Config

users passwd

Use this command to change a password. Passwords are a maximum of 64 alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If there is no password, press

enter. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Note: To specify a blank password in the configuration script, you must specify it as a space within quotes, for example, " ". For more information about creating configuration scripts, see "Configuration Scripting Commands" on page 480.

Default no password

Format **users passwd** *<username>*

Mode Global Config

no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

Format **no users passwd** *<username>*

Mode Global Config

users passwd *<username>* encrypted *<password>*

This command allows the administrator to transfer local user passwords between devices without having to know the passwords. The *<password>* parameter must be exactly 128 hexadecimal characters. The user represented by the *<username>* parameter must be a pre-existing local user.

Format **users passwd** *<username>* **encrypted** *<password>*

Mode Global Config

users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are **readonly** or **readwrite**. The *<username>* is the login user name for which the specified access mode applies. The default is **readwrite** for the "admin" user and **readonly** for all other users. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Defaults
- admin - readwrite
- other - readonly

Format **users snmpv3 accessmode** *<username> {readonly | readwrite}*

Mode Global Config

no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **readwrite** for the "admin" user and **readonly** for all other users. The *<username>* value is the user name for which the specified access mode will apply.

Format **no users snmpv3 accessmode** *<username>*

Mode Global Config

users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **none**, **md5** or **sha**. If you specify **md5** or **sha**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *<username>* is the user name associated with the authentication protocol. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Default no authentication

Format **users snmpv3 authentication** *<username> {none | md5 | sha}*

Mode Global Config

no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to **none**. The *<username>* is the user name for which the specified authentication protocol is used.

Format **no users snmpv3 authentication** *<username>*

Mode Global Config

users snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **des** or **none.**

If you select **des**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **des** protocol but do not provide a key, the user is prompted for the key. When you use the **des** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **none**, you do not need to provide a key.

The *<username>* value is the login user name associated with the specified encryption. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Default no encryption

Format **users snmpv3 encryption** *<username> {none | des[key]}*

Mode Global Config

no users snmpv3 encryption

This command sets the encryption protocol to **none**. The *<username>* is the login user name for which the specified encryption protocol will be used.

Format `no users snmpv3 encryption` *<username>*

Mode Global Config

show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format `show users`

Mode Privileged EXEC

Term	Definition
User Name	The name the user enters to login using the serial port, Telnet or Web.
Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the “admin” user has Read/Write access and the “guest” has Read Only access. There can only be one Read/Write user and up to five Read Only users.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to `ReadWrite,` the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to `ReadOnly,` the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users accounts

This command displays the local user status with respect to user account lockout and password aging.

Format `show users accounts`

Mode Privileged EXEC

Term	Definition
User Name	The local user account’s user name.
Access Mode	The user’s access level (read-only or read/write).
Lockout Status	Indicates whether the user account is locked out (true or false).
Password Expiration Date	The current password expiration date in date format.

passwd

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format `password <cr>`

Mode User EXEC

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default 8

Format `passwords min-length <8-64>`

Mode Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format `no passwords min-length`

Mode Global Config

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

Default 0

Format `passwords history <0-10>`

Mode Global Config

no passwords history

Use this command to set the password history to the default value.

Format `no passwords history`

Mode Global Config

passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default 0

Format **`passwords aging`** *`<1-365>`*

Mode Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format **`no passwords aging`**

Mode Global Config

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default 0

Format **`passwords lock-out`** *`<1-5>`*

Mode Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format **`no passwords lock-out`**

Mode Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format **`show passwords configuration`**

Mode Privileged EXEC

Term	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

Format `write memory`

Mode Privileged EXEC

CONFIGURATION

show memcard

Copy system:running-config nvram:startup-config <description> <cr> to save the current configuration with the given description.

The command “copy system:running-config nvram:startup-config <description> <cr>” would save the current configuration with the <description>.

An alternative command to copy is “write memory”, which has the same effect.

The CLI also provides the commands to upload or download the configuration files.

Download: *copy <url> nvram:startup-config*

Upload: *copy nvram:startup-config <url>*

The memory card can be cleared with the command “clear memcard”. Some Card information is displayed by using “show memcard” which results in the following output:

Show Commands in Priviledged Exec Mode for SFP, POE, SCRJ, Temperature, DHCP Relay Agent, enhanced Port Information and Time:

show sfp <slot/port> // SFP Module information

show sfp all

show poe <slot/port> // PoE Module information

show poe all

show scrj <slot/port> // POF SCRJ Module information

show scrj all

show port full <slot/port> // Display full port information

show port full all

show temperature show device temperature

show time // show internal device clock state

show ip dhcp relay-agent // show DHCP Relay Agent information

Config Commands in Priviledged Exec Mode for time settings at Real Time Clock:

time set <hour> <minute> <second> <year> <month> <day>// set internal device clock

Config Commands in Global Config Mode for SNTP and DHCP Relay Agent:

sntp manycast address <ipaddress> // set SNTP Manycast Address (should be a broadcast address)

sntp client utc-offset <-12 - 12> // set the local time zone

service dhcp-relay-agent // enable DHCP Relay Agent

no service dhcp-relay-agent // disable DHCP Relay Agent

ip dhcp relay-agent server <ipaddr> // Configure DHCP server IP address

ip dhcp relay-agent remote-id ip-address // Set the DHCP remote ID option 82 to IP Address

ip dhcp relay-agent remote-id mac-address // Set the DHCP remote ID option 82 to MAC Address

Config Commands for POE and DHCP Relay Agent in Interface Config Mode:

poe power enable // enable Power over Ethernet

no poe power enable // disable Power over Ethernet

poe current-limitation enable // enable Power over Ethernet current limitation

no poe current-limitation enable // disable Power over Ethernet current limitation

poe fault-monitoring enable // enable Power over Ethernet fault monitoring

no poe fault-monitoring enable // disable Power over Ethernet fault monitoring

ip dhcp relay-agent // enable Interface for DHCP Relay Agent

no ip dhcp relay-agent // disable Interface for DHCP Relay Agent

MRP Commands

In Global Config Mode:

MRP

domain name

manager-priority

mode

ports

vlanid

In Privileged Exec Mode:

show mrp

Spanning Tree enhanced Commands:

(no) spanning-tree large-tree-support

Format: (no) spanning-tree large-tree-support

Mode: Global Config

(no) spanning-tree fast-ring-detection

Format: (no) spanning-tree fast-ring-detection

Mode: Global Config

show spanning-tree fast-rings

Mode: Privileged EXEC, User EXEC

Ring-Number

Local Ring Ports A & B (port number)

Blocking Port of Ring Port & Mac

Status (OK, Ring Port A Failed, Broken)

Profinet Commands

Command	Additions	where	Description
operatingmode profinet	“no” cmd	config	De-/Activates the profinet mode
profinet alarm mrp	“no” cmd, Config-File	config/profinet	De-/Activates profinet alarm for MRP
profinet alarm power	“no” cmd, Config-File	config/profinet	De-/Activates profinet alarm for power supply
profinet alarm <port> link	“no” cmd, Config-File	config/profinet	De-/Activates profinet alarm for linkmonitoring on this port
profinet alarm <port > pofscrj	“no” cmd, Config-File	config/profinet	De-/Activates profinet alarm for pof scrj diagnostic on this port

Digital Input CLI commands

The following CLI commands have been implemented for digital input handling:

- show digital_input
- This command enables the user to investigate digital input status. It is available in privileged mode.

Link Monitoring CLI commands

The following CLI commands have been implemented for link monitoring handling:

- in privileged mode:
- show link-monitoring"
- in interface configuration mode:
- "link-monitoring" (enable link monitoring for this interface)
- "no link-monitoring" (disable link monitoring for this interface)

Alarm contact CLI commands

The following CLI commands have been implemented for alarm contact handling:

- alarm_contact [global | link_monitoring | mrp_ring_fault | poe_fault | port_security | power_supply] [contact_1 | contact_2]
- This command is available in privileged mode. This command enables one of the alarm contacts (depending on last parameter contact_1 or contact_2) for a special mode where special modes depend on the 1st parameter:
- global: Alarm contact is enabled globally, i.e. all it is armed for any event that might be configured separately.
- link_monitoring: If the corresponding contact is enabled globally, it will open in case of link monitoring events.
- mrp_ring_fault: If the corresponding contact is enabled globally, it will open in case of mrp ring failure event (only on MRP master!).

- poe_fault: If the corresponding contact is enabled globally, it will open in case of PoE failure event (only on MRP master!).
- port_security: If the corresponding contact is enabled globally, it will open in case of an not allowed MAC address detected at a protected port.
- power_supply: If the corresponding contact is enabled globally, it will open in case of failure of one Power Supply (US1 or US2).

SNMP COMMANDS

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *<name>*, *<loc>* and *<con>* is from 1 to 31 alphanumeric characters.

Default none

Format **snmp-server** *{sysname <name> | location <loc> | contact <con>}*

Mode Global Config

snmp-server community

This command adds (and names) a new SNMP community. A community *<name>* is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of *<name>* can be up to 16 case-sensitive characters.

Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default
- Public and private, which you can rename.
- Default values for the remaining four community names are blank.

Format **snmp-server community** *<name>*

Mode Global Config

no snmp-server community

This command removes this community name from the table. The *<name>* is the community name to be deleted.

Format **no snmp-server community** *<name>*

Mode Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default 0.0.0.0

Format **`snmp-server community ipaddr`** *`<ipaddr> <name>`*

Mode Global Config

no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format **`no snmp-server community ipaddr`** *`<name>`*

Mode Global Config

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default 0.0.0.0

Format **`snmp-server community ipmask`** *`<ipmask> <name>`*

Mode Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Format **`no snmp-server community ipmask`** *`<name>`*

Mode Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If

the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default
- private and public communities - enabled
- other four - disabled

Format `snmp-server community mode <name>`

Mode Global Config

no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format `no snmp-server community mode <name>`

Mode Global Config

snmp-server community ro

Format `snmp-server community ro <name>`

Mode Global Config

This command restricts access to switch information. The access mode is read-only (also called public).

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format `snmp-server community rw <name>`

Mode Global Config

snmp-server enable traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Note: For other port security commands, see “Protected Ports Commands” on page 31.

Default disabled

Format `snmp-server enable traps violation`

Mode Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format `no snmp-server enable traps violation`

Mode Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default enabled

Format `snmp-server enable traps`

Mode Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`

Mode Global Config

snmp-server enable traps linkmode

Note: This command may not be available on all platforms.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “snmp trap link-status” on page 37.

Default enabled

Format `snmp-server enable traps linkmode`

Mode Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format `no snmp-server enable traps linkmode`

Mode Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default enabled

Format `snmp-server enable traps multiusers`

Mode Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `no snmp-server enable traps multiusers`

Mode Global Config

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default enabled

Format `snmp-server enable traps stpmode`

Mode Global Config

no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format `no snmp-server enable traps stpmode`

Mode Global Config

snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

Example: The following shows an example of the CLI command.

```
(admin #) snmptrap mytrap ip6addr 3099::2
```

Note: The *<name>* parameter does not need to be unique, however; the *<name>* and *<ipaddr>* pair must be unique. Multiple entries can exist with the same *<name>*, as long as they are associated with a different *<ipaddr>*. The reverse scenario is also acceptable. The *<name>* is the community name used when sending the trap to the receiver, but the *<name>* is not directly associated with the SNMP Community Table, See “snmp-server community” on page39.”

Default snmpv2

Format **snmptrap** *<name> <ipaddr> [snmpversion <snmpversion>]*

Mode Global Config

no snmptrap

This command deletes trap receivers for a community.

Format **no snmptrap** *<name> <ipaddr>*

Mode Global Config

snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* parameter options are snmpv1 or snmpv2.

Note: This command does not support a “no” form.

Default snmpv2

Format **snmptrap snmpversion** *<name> <ipaddr> <snmpversion>*

Mode Global Config

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format **snmptrap ipaddr** *<name> <ipaddrold> <ipaddrnew>*

Mode Global Config

snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format **snmptrap mode** *<name> <ipaddr>*

Mode Global Config

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format `no snmptrap mode <name> <ipaddr>`

Mode Global Config

snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 34.

Format `snmp trap link-status`

Mode Interface Config

no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled.

Format `no snmp trap link-status`

Mode Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 34.

Format `snmp trap link-status all`

Mode Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 34.

Format `no snmp trap link-status all`

Mode Global Config

show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format `show snmpcommunity`

Mode Privileged EXEC

Term	Definition
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string.
Status	The status of this community access entry.

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format `show snmptrap`

Mode Privileged EXEC

Term	Definition
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.
IP Address	The IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2

Term	Definition
Mode	The receiver's status (enabled or disabled).

Example: The following shows an example of the CLI command.

```
(admin) #show snmptrap

 Community Name   IpAddress     IPv6 Address     Snmp Version    Mode
   Mytrap         0.0.0.0       2001::1          SNMPv2          Enable
show trapflags
```

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Term	Definition
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
Broadcast Storm Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPF traps' information.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPFv3 traps' information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

RADIUS COMMANDS

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default disable

Format `authorization network radius`

Mode Global Config

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format `no authorization network radius`

Mode Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format `radius accounting mode`

Mode Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format `no radius accounting mode`

Mode Global Config

radius server attribute 4

Use this command to set the NAS-IP address for the radius server.

Default Interface IP address that connects the switch to the radius server.

Format `radius server attribute 4` *`[ipaddr]`*

Mode Global Config

Term	Definition
ipaddr	A valid IP address.

no radius server attribute 4

Use this command to reset the NAS-IP address for the radius server.

Format `no radius server attribute 4`

Mode Global Config

radius server host

This command is used to configure the RADIUS authentication and accounting server. If you use the *<auth>* parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command. If you use the optional *<port>* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *<port>* number range is 1 - 65535, with 1812 being the default value.

Note: To re-configure a RADIUS authentication server to use the default UDP <*port*>, set the <*port*> parameter to 1812.

If you use the *<acct>* token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional *<port>* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a *<port>* is already configured for the accounting server, the new *<port>* replaces the previously configured *<port>*. The *<port>* must be a value in the range 1 - 65535, with 1813 being the default.

Note: To re-configure a RADIUS accounting server to use the default UDP <*port*>, set the <*port*> parameter to 1813.

Format `radius server host` *{auth | acct} <ipaddr|hostname> [<port>]*

Mode Global Config

no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used,

the previously configured RADIUS accounting server is removed from the configuration. The *<ipaddr|hostname>* parameter must match the IP address or hostname of the previously configured RADIUS authentication / accounting server.

Format **no radius server host** *{auth | acct} <ipaddress|hostname>*

Mode Global Config

radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note: The secret must be an alphanumeric value not exceeding 16 characters.

Format **radius server key** *{auth | acct} <ipaddr|hostname> [encrypted <encrypted-password>]*

Mode Global Config

Example: The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted <encrypt-string>
```

radius server msgauth

This command enables the message authenticator attribute for a specified server.

Format **radius server msgauth** *<ipaddr|hostname>*

Mode Global Config

no radius server msgauth

This command disables the message authenticator attribute for a specified server.

Format **no radius server msgauth** *<ipaddr|hostname>*

Mode Global Config

radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server handles RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. You can configure up to three servers on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address or hostname specified used in this command will become the new primary server. The IP address or hostname must match that of a previously configured RADIUS authentication server.

Format **radius server primary** *<ipaddr|hostname>*

Mode Global Config

radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Default 4

Format **radius server retransmit** *<retries>*

Mode Global Config

no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

Format **no radius server retransmit**

Mode Global Config

radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default 5

Format **radius server timeout** *<seconds>*

Mode Global Config

no radius server timeout

This command sets the timeout value to the default value.

Format **no radius server timeout**

Mode Global Config

show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items are displayed.

Format **`show radius`** *`[servers]`*

Mode Privileged EXEC

Term	Definition
Primary Server IP Address or Hostname	The configured server currently in use for authentication.
Number of configured servers	The number of configured authentication servers, including DNS configured server.
Max number of retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Timeout Duration	The configured timeout value, in seconds, for request re-transmissions.
Accounting Mode	Yes or No.

If you use the *`[servers]`* keyword, the following information displays:

Term	Definition
IP Address or Hostname	IP address or hostname of the configured RADIUS server.
Port	The port in use by this server.
Type	Primary or secondary.
Secret Configured	Yes / No.
Message Authenticator	The message authenticator attribute for the selected server, which can be enables or disables.

show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format **`show radius accounting`** *`[statistics <ipaddr|hostname>]`*

Mode Privileged EXEC

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
Mode	Enabled or disabled.
IP Address / Hostname	The configured IP address or hostname of the RADIUS accounting server.
Port	The port in use by the RADIUS accounting server.
Secret Configured	Yes or No.

If you use the optional *statistics <ipaddr|hostname>* parameter, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Term	Definition
Accounting Server IP Address / Hostname	IP address or hostname of the configured RADIUS accounting server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP address or hostname specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format **show radius statistics** *[<ipaddr|hostname>]*

Mode Privileged EXEC

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Term	Definition
Invalid Server Addresses or Hostname	The number of RADIUS Access-Response packets received from unknown addresses.
Server IP Address / Hostname	IP address or hostname of the Server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply, Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmission	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

CONFIGURATION SCRIPTING COMMANDS

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the **`show running-config`** command (see "show running-config" on page 12) to capture the running configuration into a script. Use the **`copy`** command (see "copy" on page 24) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet!Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Note: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user **jane** from a blank password to **hello**, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

This command applies the commands in the script to the switch. The *<scriptname>* parameter is the name of the script to apply.

Format **script apply** *<scriptname>*

Mode Privileged EXEC

script delete

This command deletes a specified script where the *<scriptname>* parameter is the name of the script to delete. The *<all>* option deletes all the scripts present on the switch.

Format **script delete** *{<scriptname> | all}*

Mode Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format `script list`

Mode Global Config

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which is named *<scriptname>*.

Format `script show` *<scriptname>*

Mode Privileged EXEC

Term	Definition
Output Format	`line` *<number>*`:` *<line contents>*

script validate

This command validates a script file by parsing each line in the script file where *<scriptname>* is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format `script validate` *<scriptname>*

Mode Privileged EXEC

List of Commands